



Networking the world's business data™

E / OS

Enterprise Operating System Command Line Interface User Manual

P/N 620-000134-720
REV A

Simplifying Storage Network Management

McDATA Corporation
380 Interlocken Crescent Broomfield, CO 80021-3464
Corporate Headquarters: 800-545-5773
Sales E-mail: sales@mcddata.com Web: www.mcddata.com

Record of Revisions and Updates

Revision	Date	Description
620-000134-000	11/2001	Initial release of Manual
620-000134-100	05/2002	Updates for E/OS 2.0
620-000134-200	08/2002	Updates for E/OS 3.0
620-000134-300	09/2002	Updates for E/OS 4.0
620-000134-400	10/2002	Updates for E/OS 4.1
620-000134-500	10/2002	Updates for E/OS 4.1 CD-ROM final
620-000134-600	2/2003	Updates for E/OS 5.1 and EFCM 7.1
620-000134-601	7/2003	Updates for E/OS 5.5
620-000134-700	10/2003	Updates for E/OS 6.0
620-000134-710	12/2003	Updates for E/OS 6.1
620-000134-720	6/2004	Updates for E/OS 6.2
620-000134-730	01/2005	Updates for E/OS 7.0

Copyright © 2001 - 2004 McDATA Corporation. All rights reserved.

Printed December 2004

First Edition

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written consent of McDATA Corporation. The information contained in this document is subject to change without notice. McDATA Corporation assumes no responsibility for any errors that may appear.

All computer software programs, including but not limited to microcode, described in this document are furnished under a license, and may be used or copied only in accordance with the terms of such license. McDATA either owns or has the right to license the computer software programs described in this document. McDATA Corporation retains all rights, title and interest in the computer software programs.

McDATA Corporation makes no warranties, expressed or implied, by operation of law or otherwise, relating to this document, the products or the computer software programs described herein. McDATA CORPORATION DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. In no event shall McDATA Corporation be liable for (a) incidental, indirect, special, or consequential damages or (b) any damages whatsoever resulting from the loss of use, data or profits, arising out of this document, even if advised of the possibility of such damages.

©2004 McDATA Corporation. All rights reserved. McDATA, the McDATA logo, McDATA Eclipse, Fabriccenter, HotCAT, Intrepid, Multi-Capable Storage Network Solutions, Networking the World's Business Data, nScale, nView, OPENready, SANavigator, SANpilot, SANtegrity, SANvergence, SecureConnect and Sphereon are trademarks or registered trademarks of McDATA Corporation. OEM and Reseller logos are the

property of such parties and are reprinted with limited use permission. All other trademarks are the property of their respective companies. All specifications subject to change.



Preface	xv
----------------------	----

Chapter 1 Introduction

Command Line Interface Overview.....	1-2
Entering Command Line Interface Commands	1-3
Documentation Conventions.....	1-3
Navigation Conventions.....	1-3
Command Tree.....	1-5
Navigation of the CLI Command Tree	1-12
Parameters	1-13
Output	1-14
Logging In and Logging Out	1-14
User Access Rights	1-14
Passwords and Secrets	1-14
login	1-15
logout.....	1-16
Using the commaDelim Command.....	1-17
commaDelim	1-17
Handling Command Line Interface Errors	1-18
Using the Command Line Interface Help	1-19
Commenting Scripts	1-20
ED-5000 Director	1-21
Telnet Session.....	1-22
Ethernet Connection Loss.....	1-22
Backup and Restoration	1-23

Chapter 2 CLI Commands

Command Overview	2-2
------------------------	-----

New and Changed Commands	2-2
config	2-5
config.enterpriseFabMode.setState	2-5
config.features.enterpriseFabMode	2-6
config.features.ficonMS	2-6
config.features.installKey	2-7
config.features.NPIV	2-8
config.features.openSysMS	2-8
config.features.openTrunking	2-8
config.features.show	2-9
config.fencing.addPolicy	2-10
config.fencing.addPort	2-10
config.fencing.deletePolicy	2-11
config.fencing.removePort	2-12
config.fencing.setParams	2-12
config.fencing.setState	2-14
config.fencing.show	2-14
config.fencing.showTypeTable	2-16
config.ficonCUPZoning.addControlHost	2-16
config.ficonCUPZoning.deleteControlHost	2-17
config.ficonCUPZoning.setState	2-17
config.ficonCUPZoning.show	2-18
config.ficonMS.setMIHPTO	2-18
config.ficonMS.setState	2-19
config.ficonMS.show	2-20
config.ip.ethernet	2-20
config.ip.lineSpeed	2-21
config.ip.show	2-21
config.NPIV.maxPortIDs	2-22
config.NPIV.setState	2-23
config.NPIV.show	2-23
config.openSysMS.setHostCtrlState	2-24
config.openSysMS.setState	2-24
config.port.blocked	2-25
config.port.fan	2-25
config.port.name	2-26
config.port.rxCredits	2-26
config.port.show	2-27
config.port.showPortAddr	2-28
config.port.speed	2-29
config.port.swapPortByAddr	2-30
config.port.swapPortByNum	2-30
config.port.type	2-31

config.security	2-32
config.security.authentication.interface api.outgoing	2-33
config.security.authentication.interface.api.sequence	2-33
config.security.authentication.interface.cli.sequence	2-34
config.security.authentication.interface.eport.outgoing ...	2-34
config.security.authentication.interface.eport.sequence ...	2-35
config.security.authentication.interface.nport.outgoing ...	2-36
config.security.authentication.interface.nport.sequence ...	2-36
config.security.authentication.interface.osms.outgoing ...	2-37
config.security.authentication.interface.osms.setKey	2-38
config.security.authentication.interface.serial. enhancedAuth	2-38
config.security.authentication.interface.show	2-39
config.security.authentication.interface.web.sequence	2-39
config.security.authentication.port.override	2-40
config.security.authentication.port.show	2-41
config.security.authentication.RADIUS.attempts	2-42
config.security.authentication.RADIUS.deadtime	2-42
config.security.authentication.RADIUS.deleteServer	2-43
config.security.authentication.RADIUS.server	2-43
config.security.authentication.RADIUS.show	2-44
config.security.authentication.RADIUS.timeout	2-45
config.security.authentication.switch.setSecret	2-45
config.security.authentication.user	2-46
config.security.authentication.user.add	2-46
config.security.authentication.user.delete	2-47
config.security.authentication.user.modify	2-48
config.security.authentication.user.role	2-49
config.security.authentication.user.show	2-50
config.security.fabricBinding	2-51
config.security.fabricBinding.activatePending	2-53
config.security.fabricbinding.addAttachedMembers	2-53
config.security.fabricBinding.addMember	2-54
config.security.fabricBinding.clearMemList	2-54
config.security.fabricbinding.deactivateFabBind	2-55
config.security.fabricBinding.deleteMember	2-55
config.security.fabricBinding.replacePending	2-56
config.security.fabricBinding.showActive	2-56
config.security.fabricBinding.showPending	2-57
config.security.portBinding	2-57
config.security.portBinding.bound	2-57
config.security.portBinding.show	2-58
config.security.portBinding.wwn	2-59

config.security.ssh.resetKeys	2-61
config.security.ssh.setState.....	2-61
config.security.ssh.show	2-61
config.security.switchAcl	2-62
config.security.switchAcl.addRange	2-62
config.security.switchAcl.deleteRange	2-63
config.security.switchAcl.setState.....	2-63
config.security.switchAcl.show	2-64
config.security.switchBinding	2-64
config.security.switchBinding.addMember	2-65
config.security.switchBinding.deleteMember.....	2-66
config.security.switchBinding.setState.....	2-66
config.security.switchBinding.show	2-67
config.snmp.addCommunity.....	2-68
config.snmp.authTraps.....	2-69
config.snmp.deleteCommunity	2-70
config.snmp.setFaMibVersion	2-70
config.snmp.setState	2-71
config.snmp.show	2-71
config.switch	2-72
config.switch.domainRSCN.....	2-72
config.switch.edTOV.....	2-73
config.switch.insistDomainId	2-73
config.switch.interopMode	2-74
config.switch.ltdFabRSCN	2-74
config.switch.prefDomainId	2-75
config.switch.priority	2-75
config.switch.raTOV	2-76
config.switch.rerouteDelay	2-77
config.switch.speed	2-78
config.switch.show	2-78
config.switch.zoneFlexPars.....	2-80
config.switch.zoningRSCN	2-81
config.system.contact	2-81
config.system.date	2-82
config.system.description.....	2-82
config.system.location	2-83
config.system.name.....	2-83
config.system.show	2-83
config.zoning.....	2-84
config.zoning.activateZoneSet.....	2-85
config.zoning.addPortMem	2-86
config.zoning.addWwnMem	2-87

config.zoning.addZone	2-87
config.zoning.clearZone	2-88
config.zoning.clearZoneSet	2-88
config.zoning.deactivateZoneSet	2-89
config.zoning.deletePortMem	2-89
config.zoning.deleteWwnMem	2-90
config.zoning.deleteZone	2-90
config.zoning.renameZone	2-91
config.zoning.renameZoneSet	2-91
config.zoning.replaceZoneSet	2-92
config.zoning.setDefZoneState	2-92
config.zoning.showActive	2-92
config.zoning.showPending	2-93
maint	2-95
maint.port.beacon	2-95
maint.port.reset	2-96
maint.system.beacon	2-96
maint.system.clearSysError	2-97
maint.system.ipl	2-97
maint.system.resetConfig	2-97
maint.system.setOnlineState	2-98
perf	2-99
perf.class2	2-99
perf.class3	2-100
perf.clearStats	2-102
perf.errors	2-102
perf.link	2-104
perf.openTrunking.backPressure	2-105
perf.openTrunking.congestionThresh	2-106
perf.openTrunking.lowBBCreditThresh	2-106
perf.openTrunking.setState	2-107
perf.openTrunking.show	2-108
perf.openTrunking.unresCongestion	2-109
perf.preferredPath	2-110
perf.preferredPath.clearPath	2-110
perf.preferredPath.setPath	2-111
perf.preferredPath.setState	2-112
perf.preferredPath.showPath	2-113
perf.preferredPath.showState	2-115
perf.thresholdAlerts	2-116
perf.thresholdAlerts.counter.addAlert	2-120
perf.thresholdAlerts.counter.addPort	2-121
perf.thresholdAlerts.counter.removePort	2-122

perf.thresholdAlerts.counter.setCounter	2-123
perf.thresholdAlerts.counter.setParams	2-124
perf.thresholdAlerts.counter.show	2-125
perf.threshholdAlerts.counter.showStatisticTable	2-126
perf.thresholdAlerts.deleteAlert	2-127
perf.thresholdAlerts.setState	2-127
perf.thresholdAlerts.show	2-127
perf.thresholdAlerts.throughput.addAlert	2-129
perf.thresholdAlerts.throughput.addPort	2-130
perf.thresholdAlerts.throughput.removePort	2-131
perf.thresholdAlerts.throughput.setUtilType	2-132
perf.thresholdAlerts.throughput.setUtilPercentage	2-133
perf.thresholdAlerts.throughput.setParams	2-134
perf.thresholdAlerts.throughput.show	2-135
perf.thresholdAlerts.throughput.showUtilTypeTable	2-135
perf.traffic	2-136
show	2-138
show.all	2-138
show.auditLog	2-139
show.epFrameLog.config	2-140
show.epFrameLog.filterClassFFrames	2-140
show.epFrameLog.setFilterPort	2-141
show.epFrameLog.noWrap	2-142
show.epFrameLog.wrap	2-143
show.eventLog	2-144
show.fabricLog.noWrap	2-145
show.fabricLog.wrap	2-146
show.fabric.nodes	2-148
show.fabric.principal	2-148
show.fabric.topology	2-149
show.features	2-150
show.fencing.policies	2-150
show.ficonCUPZoning	2-152
show.ficonMS	2-152
show.frus	2-153
show.ip.ethernet	2-154
show.linkIncidentLog	2-154
show.loginServer	2-155
show.nameServer	2-156
show.nameServerExt	2-158
show.NPIV.config	2-159
show.openSysMS.config	2-160
show.openTrunking.config	2-161

show.openTrunking.rerouteLog..... 2-162

show.port.config 2-163

show.port.exit 2-164

show.port.info 2-166

show.port.nodes..... 2-167

show.port.opticEDD 2-169

show.port.opticInfo 2-170

show.port.profile..... 2-171

show.port.showPortAddr 2-173

show.port.status 2-174

show.port.technology 2-177

show.preferredPath.showPath..... 2-178

show.security.fabricBinding..... 2-180

show.security.log 2-181

show.security.portBinding 2-182

show.security.switchAcl 2-183

show.security.switchBinding 2-184

show.snmp 2-185

show.switch 2-186

show.system..... 2-188

show.thresholdAlerts.alerts..... 2-189

show.thresholdAlerts.log..... 2-192

show.zoning..... 2-194

Appendix A Error Messages

Appendix B Commands and Corresponding Releases

Glossary g-1

Index i-1

1-1	CLI Command Tree Navigation Conventions	1-3
1-2	CLI Command Tree	1-5
1-3	CLI Command Tree for the ED-5000 Director	1-21
2-1	Supported Zoning Configurations	2-85
2-2	Throughput Threshold Alerts	2-118
2-3	Alert Counters	2-118
B-1	Commands and Releases	B-1

This publication is part of the documentation suite that supports the McDATA® Sphereon™ 3016 Fabric Switch, Sphereon 3032 Fabric Switch, Sphereon 3216 Fabric Switch, Sphereon 3232 Fabric Switch, Sphereon 4300 Fabric Switch, Sphereon 4500 Fabric Switch, Intrepid® 6064 Director, and Intrepid 6140 Director.

Who Should Use This Manual

This publication describes the commands that can be entered through the Command Line Interface (CLI) for the Intrepid® 6064 Director, and Intrepid 6140 Director, Sphereon™ 3016 Switch, Sphereon 3032 Switch, Sphereon 3216 Switch, Sphereon 3232 Switch, Sphereon 4300 Switch, and Sphereon 4500 Switch. (A limited number of these commands are available on the ED-5000 Director.) Access through a Telnet client is presumed.

This publication is intended for data center administrators and customer support personnel, who can either enter the commands manually or write a script containing them. However, the primary purpose of the Command Line Interface is for scripts written by these administrators and personnel for use in a host-based scripting environment. Therefore, this publication presumes that the user is familiar with:

- Establishing and using a Telnet session
- Using the command line of a terminal
- Writing scripts
- Networking, SAN, and zoning concepts
- McDATA products in the user's network

The publications listed in [Related Publications](#) provide considerable information about both concepts and McDATA products.

Organization of This Manual

This publication is organized as follows:

- [Chapter 1, Introduction](#), provides an introduction and overview of the Command Line Interface.
- [Chapter 2, CLI Commands](#), describes the Command Line Interface commands, including their syntax, purpose, and parameters, as well as examples of their usage and any output that they generate.
- [Appendix A, Error Messages](#) lists and explains error messages that may appear while using the CLI.
- [Appendix B, Commands and Corresponding Releases](#) lists each command in the CLI and the release in which the command was added to the CLI.
- The [Glossary](#) defines terms, abbreviations, and acronyms used in this manual.
- An [Index](#) is also provided.

Manual Updates

Check the McDATA web site at www.mcdata.com for possible updates or supplements to this manual.

Related Publications

Other publications that provide additional information about the products mentioned in this manual are:

- *Configuration Backup and Restore Utility Installation and User Guide* (958-000370)
- *Products in a SAN Environment - Planning Manual* (620-000124)
- *McDATA ED-5000 Director Element Manager User Manual* (620-000176)
- *Intrepid 6064 Director Installation and Service Manual* (620-000108)
- *Intrepid 6140 and 6064 Directors Element Manager User Manual* (620-000172)
- *Intrepid 6140 Director Installation and Service Manual* (620-000157)
- *E/OSn SNMP Support Manual* (620-000226)
- *SANpilot User Manual* (620-000160)

- *Sphereon 3016 and 3216 Fabric Switch Element Manager User Manual* (620-000174)
- *Sphereon 3016 and 3216 Fabric Switches Installation and Service Manual* (620-000154)
- *Sphereon 3032 and 3232 Fabric Switch Element Manager User Manual* (620-000173)
- *Sphereon 3032 and 3232 Fabric Switches Installation and Service Manual* (620-000155)
- *Sphereon 4300 Fabric Switch Installation and Service Manual* (620-000171)
- *Sphereon 4500 Fabric Switch Installation and Service Manual* (620-000159)
- *Sphereon 4500 Fabric Switch Element Manager User Manual* (620-000175)

Manual Conventions

The following notational conventions are used in this document:

Convention	Meaning
Bold	Keyboard keys, buttons and switches on hardware products, and screen prompts for the Command Line Interface.
<i>Italic</i>	Outside book references, names of user interface windows, buttons, and dialog boxes.
Monospaced	Command syntax, examples of commands, output.

NOTE: A note presents important information that is not hazard-related.

ATTENTION! An attention notice presents important information about activities that could result in loss of equipment function or loss of data.

Where to Get Help

For technical support, McDATA end-user customers should call the phone number located on the service label attached to the front or rear of the hardware product.

For IBM products, contact IBM for technical support, which includes hardware support, all product repairs, and ordering of spare parts.

Go to:

<http://www.ibm.com/servers/storage/support/san/index.html>.

McDATA's "Best in Class" Solution Center provides a single point of contact for customers seeking help with McDATA software products. The Solution Center will research, explore, and resolve inquiries or service requests regarding McDATA products and services. The Solution Center is staffed 24 hours a day, 7 days a week, including holidays.

NOTE: To expedite warranty entitlement, please have your product serial number available.

McDATA Corporation
380 Interlocken Crescent
Broomfield, CO 80021

Phone: (800) 752-4572 or (720) 558-3910

Fax: (720) 558-3581

E-mail: support@mcddata.com

NOTE: Customers who purchased the hardware product from a company other than McDATA should contact that company's service representative for technical support.

Forwarding Publication Comments

We sincerely appreciate any comments about this publication. Did you find this manual easy or difficult to use? Did it lack necessary information? Were there any errors? Could its organization be improved?

Please send your comments via e-mail, our home page, or FAX. Identify the manual, and provide page numbers and specific detail. Thank you.

E-mail: pubsmgr@mcddata.com

Home Page: <http://www.mcddata.com>

Fax: Technical Communications Manager
(720) 558-8999

Ordering Publications

To order a paper copy of this manual, contact your McDATA representative, or use the contact information listed below.

Phone: (800) 545-5773 and select the option for information on McDATA's complete family of enterprise-to-edge SAN solutions.

Fax: (720) 558-4193

Trademarks The following terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of McDATA Corporation in the United States, other countries, or both:

<u>Registered Trademarks</u>	<u>Trademarks</u>
Fabricenter®	E/OS™
HotCAT®	Eclipse™
Intrepid®	Fibre Channel Director™
McDATA®	OPENconnectors™
OPENready®	SANvergence™
SANavigator®	Sphereon™
SANpilot®	
SANtegrity®	

All other trademarked terms, indicated by a registered trademark symbol (®) or trademark symbol (™) on first use in this publication, are trademarks of their respective owners in the United States, other countries, or both.

This chapter introduces the Command Line Interface (CLI) and describes the essentials for using the CLI commands.

- *Command Line Interface Overview* 1-2
- *Entering Command Line Interface Commands* 1-3
- *Logging In and Logging Out* 1-14
- *Using the commaDelim Command* 1-17
- *Handling Command Line Interface Errors* 1-18
- *Using the Command Line Interface Help* 1-19
- *Commenting Scripts* 1-20
- *ED-5000 Director* 1-21
- *Telnet Session* 1-22
- *Backup and Restoration* 1-23

Command Line Interface Overview

The Command Line Interface (CLI) is a feature that provides an alternative to Graphical User Interface (GUI) and web-based (HTTP) interface products for director and switch management capabilities.

The CLI can only be used through a Telnet client session in an out-of-band management environment, using the Ethernet port in the director or switch. Although the primary use of the CLI is in host-based scripting environments, the CLI commands can also be entered directly at a command line. Any hardware platform that supports the Telnet client software can be used.

The primary purpose of the CLI is to automate management of a large number of switches with the use of scripts.

Because the CLI is not an interactive interface, no prompts are displayed to guide the user through a task. If an interactive interface is needed, use the GUI-based or web-based SAN management applications instead of the CLI.

Entering Command Line Interface Commands

The CLI commands can be entered directly at the command line of a terminal or coded in a script.

Note that the CLI commands are not case sensitive.

Documentation Conventions

Throughout this publication, periods are used to separate the components of a command name. However, the periods cannot be included when the command is actually entered at the terminal or coded in a script. (How to enter the commands is explained in [Navigation of the CLI Command Tree](#) on page 1-12.)

Even though the commands cannot be entered with the periods, the command line prompts do include the periods.

Config.Port>

Navigation Conventions

Basic command line navigation conventions are supported. The following table includes the asynchronous commands that are recognized by the CLI.

Table 1-1 CLI Command Tree Navigation Conventions

Character Sequence	Common Name	Action or Description
<CR>	Carriage Return	Pass a completed line to the parser.
	Delete	Backspace one character and delete the character.
<NL>	New Line	Pass a completed line to the parser.
<SP>	Space	Used to separate keywords.
#	Pound Sign	Used to designate comments in a script.
?	Question Mark	Provide help information.
"	Quotation Mark	Used to surround a single token.
^A	Control-A	Position the cursor to the start of the line.

Table 1-1 CLI Command Tree Navigation Conventions (Continued)

Character Sequence	Common Name	Action or Description
^B	Control-B	Position the cursor left one character.
^D	Control-D	Delete the current character.
^E	Control-E	Position the cursor to the end of the line.
^F	Control-F	Position the cursor right one character.
^H	Control-H	Backspace one character and delete the character.
^I	Tab	Complete the current keyword.
^K	Control-K	Delete to the end of the line.
^L	Control-L	Redraw the line.
^N	Control-N	Move down one line in the command history.
^P	Control-P	Move up one line in the command history.
^R	Control-R	Redraw the line.
^U	Control-U	Clear the input and reset the line buffer.
^X	Control-X	Clear the input and reset the line buffer.
<ESC>[A	Up Arrow	Move up one line in the command history.
<ESC>[B	Down Arrow	Move down one line in the command history.
<ESC>[C	Right Arrow	Position the cursor right one character.
<ESC>[D	Left Arrow	Position the cursor left one character.

Command Tree

The command tree of the CLI begins from the root. [Table 1-2](#) shows the CLI command tree. The commands in the four extended branches (config, maint, perf, and show) are described in [Chapter 2, CLI Commands](#).

The following commands are not listed in the command tree, but are globally available and are documented in this chapter:

- login (see [login](#) on page 1-15)
- logout (see [logout](#) on page 1-16)
- commaDelim (see [Using the commaDelim Command](#) on page 1-17)

[Table 1-2](#) shows the command tree hierarchy from the root, reading from left to right.

Table 1-2 CLI Command Tree

config-----	enterpriseFabMode---	setState
	features -----	enterpriseFabMode
		ficonMS
		installKey
		NPIV
		openSysMS
		openTrunking
		show
	fencing-----	addPolicy
		addPort
		deletePolicy
		removePort
		setParams
		setState
		show
		showTypeTable
	ficonCUPZoning-----	addControlHost
		deleteControlHost
		setState
		show
	ficonMS-----	setMIHPTO
		setState
		show

Table 1-2 CLI Command Tree (Continued)

ip-----	ethernet				
	lineSpeed				
	show				
	setHostCtrlState				
NPIV-----	maxPortIDs				
	setState				
	show				
openSysMS-----	setState				
port -----	blocked				
	fan				
	name				
	rxCredits				
	show				
	showPortAddr				
	speed				
	swapPortByAddr				
	swapPortByNum				
	type				
security-----	authentication-----	interface-----	api-----	outgoing	
				sequence	
			cli-----	sequence	
			eport-----	outgoing	
				sequence	
			nport-----	outgoing	
				sequence	
			osms-----	outgoing	
				setKey	
			serial-----	enhancedAuth	
			show		
			web-----	sequence	
		port-----	override		
			show		
		radius-----	attempts		
			deadtime		
			deleteServer		
			server		

Table 1-2 CLI Command Tree (Continued)

		show
		timeout
	switch-----	setSecret
	user-----	add
		delete
		modify
		role
		show
security -----	fabricBinding -----	activatePending
		addAttachedMembers
		addMember
		clearMemList
		deactivateFabBind
		deleteMember
		replacePending
		showActive
		showPending
	portBinding -----	bound
		show
		wwn
	ssh-----	resetKeys
		setState
		show
	switchAcl-----	addRange
		deleteRange
		setState
		show
	switchBinding -----	addMember
		deleteMember
		setState
		show
	acl -----	addRange
		deleteRange
		setState
		show
snmp -----	addCommunity	

Table 1-2 CLI Command Tree (Continued)

	authTraps
	deleteCommunity
	setFaMibVersion
	setState
	show
switch -----	domainRSCN
	edTOV
	insistDomainId
	interopMode
	ltdFabRSCN
	prefDomainId
	priority
	raTOV
	rerouteDelay
	speed
	show
	zoneFlexPars
	zoningRSCN
system -----	contact
	date
	description
	location
	name
	show
zoning -----	setDefZoneState
	activateZoneSet
	deactivateZoneSet
	replaceZoneSet
	clearZoneSet
	addZone
	deleteZone
	renameZoneSet
	addWwnMem
	addPortMem
	clearZone
	deleteWwnMem

Table 1-2 CLI Command Tree (Continued)

		deletePortMem	
		renameZone	
		showPending	
		showActive	
<hr/>			
maint -----	port -----	beacon	
		reset	
	system -----	beacon	
		clearSysError	
		ipl	
		resetConfig	
		setOnlineState	
<hr/>			
perf -----	class2		
	class3		
	clearStats		
	errors		
	link		
	openTrunking -----	backPressure	
		congestionThresh	
		lowBBCreditThresh	
		setState	
		show	
		unresCongestion	
	preferredPath -----	clearPath	
		setPath	
		setState	
		showPath	
		showState	
	thresholdAlerts -----	counter -----	addAlert
			addPort
			removePort
			setCounter
			setParams
			show
			showStatisticTable
		deleteAlert	
		setState	

Table 1-2 CLI Command Tree (Continued)

	show	
	throughput -----	addAlert
		addPort
		removePort
		setUtilType
		setUtilPercentage
		setParams
		show
		showUtilTypeTable
	traffic	
show -----	all	
	auditLog	
	epFrameLog-----	config
		filterClassFFrames
		noWrap
		setFilterPort
		wrap
	eventLog	
	fabric-----	nodes
		principal
		topology
	fabricLog-----	noWrap
		wrap
	features	
	fencing-----	policies
	ficonCUPZoning	
	ficonMS	
	frus	
	ip -----	ethernet
	linkIncidentLog	
	loginServer	
	nameServer	
	nameServerExt	
	NPIV-----	config
	openSysMS-----	config

Table 1-2 CLI Command Tree (Continued)

openTrunking -----	config
	rerouteLog
port -----	config
	exit
	info
	nodes
	opticEDD
	opticInfo
	profile
	showPortAddr
	status
	technology
preferredPath -----	showPath
security-----	fabricBinding
	log
	log
	portBinding
	switchAcl
	switchBinding
snmp	
switch	
system	
thresholdAlerts-----	alerts
	log
zoning	

Note that the commands are shown, with the exception of the zoning commands, in alphabetical order to make them easier to locate. Although the commands can be entered in any order, depending on the results desired, the order shown in [Table 1-2, CLI Command Tree](#), page 1-5 for the zoning commands is a typical order in which the zoning commands are entered.

Note that the order in which commands are entered determines the order in which the show commands display the values. Refer to [Chapter 2, CLI Commands](#) for examples of show commands output.

Navigation of the CLI Command Tree

Once the administrator or operator logs in and receives the Root> prompt, the CLI commands are accessed by navigating up and down the CLI command tree.

To move from the root through the any of the four extended branches, enter the name of the next branch as shown in [Table 1-2, CLI Command Tree](#), page 1-5. For example, to use the config.port.name command to configure the name for port 4 on the switch, this series of commands is entered:

```
Root> config
Config> port
Config.Port> name 4 "Sam's Tape Drive"
```

At this point, to enter the maint.port.beacon command to set the beaconing state of port 4, the following series of commands is entered:

```
Config.Port> ..
Config> ..
Root> maint
Maint> port
Maint.Port> beacon 4 true
```

Note that you must return all the way to the root of the tree to transition to another extended branch. When traversing back to the root, the name of each branch cannot be used. Instead use the double-dot command (two periods) to move back towards the root. Note that only one double-dot command may be entered at a time.

One approach to making the navigation more concise is to use the root command to jump directly to the root of the CLI command tree. The previous example, which shows stepping back to the root with the double-dot command, is simplified as follows:

```
Config.Port> root
Root> maint
Maint> port
Maint.Port> beacon 4 true
```

Another approach to making the navigation more concise is to use the complete command syntax from the Root> prompt each time. For example, to issue the config.port.name command and then the maint.port.beacon command, the commands are entered as follows:

```
Root> config port name 4 "Sam's Tape Drive"
Root> maint port beacon 4 true
```


As shown in this example, use of the complete command syntax avoids navigating up and down the branches of the CLI command tree, and the prompt stays at the root. The use of complete command syntax is particularly useful when writing scripts.

When coding a script, remember to code the appropriate character sequences, which are described in [Navigation Conventions](#) on page 1-3.

```
Root> config port name 4 "Sam's Tape Drive"<CR>
Root> maint port beacon 4 true<CR>
```

Limitation on Movements

As the commands are entered, they are recorded in a history log. Note these limitations on movement that result from use of the history log:

- If a command has more than 60 characters, the command runs, but the command is not recorded in the history log, and the position in the tree does not change, as shown in the following example. Because the command is not recorded in the history, a subsequent asynchronous command (navigation command) cannot depend on it.

```
Root> config zoning addWwnMem TheUltimateZone 10:00:00:00
:C9:22:9B:64
Root>
```

- Whenever the position in the CLI command tree moves to a new branch (for example, config to maint, config to config.port, or config.port to config), the history log is cleared. In this case, any asynchronous commands (for example, the up-arrow command <ESC>[A or the up-arrow keyboard symbol) cannot move the position back towards the root, as shown in this example:

```
Root> config
Root.Config> port
Root.Config.Port> <ESC>[A
Root.Config.Port>
```

Parameters

Some command parameters accept character strings that include spaces. Quotation marks are required when a string includes spaces.

```
Config.System> location Building_24_Room_16
```

```
Config.System> location "Building 24 Room 16"
```

If spaces are not included in a parameter that accepts a string, the quotation marks are not required around that string.

To include quotation marks in a string, use the escape character (\) before the quotation marks.

Config.System> location "Building 24 \"Joe's PlayLab\""
A null string can be created by using the quotation marks without any space between them.

Config.System> location ""

Output

All output from the CLI commands is limited to the standard 80 columns supported by most Telnet interfaces. The output is left-justified.

Logging In and Logging Out

The CLI allows a single Telnet client to be connected to the switch. If a Telnet client logs out, or if after 15 minutes of inactivity the client's access times out, another Telnet client may log in. Also note that the Telnet client (user) must log in any time the director or switch is restarted because the current user's access is lost. Examples of a restart include an IPL and any power-off situation.

User Access Rights

The CLI supports two user access rights: administrator and operator. A user who logs in with administrator access rights can use all of the commands described in this publication. Operator access rights grant permission to use only the perf and show branches of the CLI command tree (for example, the perf.traffic and show.system commands) with the following exceptions: operator rights cannot access the show.preferredPath, show.security, and show.thresholdAlerts commands. Operators can also execute the globally available commands (login, logout, and commaDelim).

Passwords and Secrets

Some commands require the user to enter a password or secret before the command can be executed.

Passwords can be ASCII characters in the range of 32 to 126.

Secrets can be any ASCII character (0-255). Non-printable and extended ASCII characters can be entered by using a backslash. Two

hexadecimal characters must follow the backslash. All printable ASCII characters can be entered using the keyboard or using its hexadecimal value except for the backslash character. If a backslash is desired as part of the password its hexadecimal representation must be used. Spaces are valid, but if they appear at the begging of the password then they will be ignored. The following are examples of valid secrets.

```
simplesecret****
```

This is an example of a secret that does not use any special characters.

```
\40\72\A3\F9\12\13\14\15\16\17\18\19\55\33\87\42
```

This is an example of a secret of length 4 that is configured using the hexadecimal representation.

```
a9p\40\40xx\44\88kutfe\89h
```

This is an example of a secret that has a length of 7 characters that are composed of a mix using hexadecimal and the printable ASCII characters.

login

Syntax	login
Purpose	This command allows a Telnet client to connect to the switch.
Description	<p>This command allows the user to log in with either administrator or operator access rights. The default passwords are <i>password</i>.</p> <p>The login command is called automatically by the CLI each time a new Telnet session is activated, as well as each time new administrator access rights are configured.</p> <p>After the login command is issued, the Username: prompt automatically displays. After a valid user name is entered, the Password: prompt automatically displays. After the corresponding valid password is entered, the Root> prompt displays. At this prompt the user may enter any of the commands included in Table 1-2, CLI Command Tree, page 1-5.</p> <p>When users are prompted to change the password when logging in, they can enter the default password (<i>password</i>). This will be accepted. However, at the next login, they will again be required to change the password, if the default password is still being used. When the user</p>

enters the default password when prompted to change the password, the data portion of the security log entry for CLI login includes “password not changed.”

A user name and password can be set by the administrator through the `config.security.authentication.user.add` command or through the `config.security.authentication.user.modify` command.

The access rights chosen for the CLI are completely independent of the other product interfaces, for example, SNMP or McDATA product interfaces.

Parameters This command has no parameters.

Command Examples

```
login
Username: Administrator
Password: password

login
Username: Operator
Password: password
```

logout

Syntax `logout`

Purpose This command allows a Telnet client to disconnect from the switch.

Description This command logs out the single Telnet client connected to the switch. This command can be entered at any point in the command tree.

Parameters This command has no parameters.

Command Examples

```
Root> logout

Config> logout

Config.Port> logout
```

Using the commaDelim Command

Note that the output examples shown in the other sections of this publication presume that commaDelim is off.

commaDelim

Syntax commaDelim enable

Purpose This command enables the user to obtain displayed information in comma-delimited, rather than tabular, format. Tabular format is the default.

Description This command can be entered at any point in the command tree.

Parameter This command has one parameter

enable Specifies the comma-delineated state for output. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command Examples **Root>** commaDelim true

Config> commaDelim 1

Config.Port> commaDelim false

Output Example Output displayed in commaDelim mode is as follows:

```
Root> show eventLog
Date/Time,Code,Severity,FRU,Event Data,
04/12/01 10:58A,375,Major,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
04/12/01 10:58A,375,Major,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
04/12/01 9:58A,385,Severe,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
04/11/01 7:18P,395,Severe,CTP-0,00010203 04050607 08090A0B 0C0D0E0F,
```

Handling Command Line Interface Errors

Two types of errors detected by the CLI are:

- An error associated with the interface. For example, a keyword is misspelled or does not exist.

```
Root> config
Error 234: Invalid Command
```

- An error associated with fabric or switch issues. For example, a parameter error is detected by the switch, where port 24 is entered for a switch that supports only 16 ports.

```
Root> config port name 24 "Port 24"
Error 218: Invalid Port Number
```

In either case, the command is ignored. The CLI remains at the point it was before the command was entered.

The error messages, including error number and error, are listed in [Appendix A, Error Messages](#).

Using the Command Line Interface Help

The question mark (?) can be used within a command to obtain certain information:

- If the question mark is used in place of a command keyword, all the keywords at that level of the CLI command tree display.

```
Root> config system ?  
Command identified  
contact          - Set the system contact attribute  
date             - Set the system date and time  
description      - Set the system description attribute  
location         - Set the system location attribute  
name             - Set the system name attribute  
show            - Display the system configuration
```

- If the question mark is used at the end of a recognized command, any parameters for that command display.

```
Root> config port name ?  
- name <portNumber> <portName>
```

- If the question mark is used after one or more characters of a keyword, any keywords at that level of the CLI command tree display.

```
Root> config s?  
security snmp switch system
```

Commenting Scripts

The pound sign (#) can be used to add comments in a script file. The pound sign must be the first character in the line; the CLI ignores everything after the pound sign in that line. The following lines are valid:

```
Root> #Change port 3 to an E_Port<CR>
Root> config port<CR>
config.port> #####<CR>
config.port> ## Begin Script ##<CR>
config.port> #####<CR>
```

The pound sign cannot be used after any other characters (a command, for example) to start a comment. The following is an invalid script line:

```
Root> maint system beacon true # Turn on beaconing<CR>
```

To correct the previous script line, move the comment either before or after the line with the command. For example, the following examples are both valid:

```
Root> # Turn on beaconing<CR>
Root> maint system beacon true<CR>

Root> maint system beacon true<CR>
Root> # Turn on beaconing<CR>
```

ATTENTION! Comments of over 200 characters in length may cause unpredictable system behavior. Limit comments to 200 characters per line.

ED-5000 Director

A subset of the CLI commands described in this publication are available on the ED-5000 Director™. The globally available commands (login, logout, and commaDelim) are described previously in this chapter. The following config, maint, and show commands are described in [Chapter 2, CLI Commands](#).

Table 1-3 CLI Command Tree for the ED-5000 Director

config -----	security -----	userRights -----	administrator
			operator
			show
maint -----	system -----	resetConfig	
show -----	ip -----	ethernet	
	port -----	config	
		info	
		status	
	switch		
	system		
	zoning		

Telnet Session

The CLI can be accessed through a Telnet client session in an out-of-band management environment, using the Ethernet port in the director or switch. It can also be accessed using Secure Shell (SSH).

Although the primary use of the CLI is in host-based scripting environments, the CLI commands can also be entered directly at a command line. Any hardware platform that supports the Telnet client software can be used.

NOTE: You can use the Configure option in the GUI-based or web-based interfaces to enable/disable Telnet access. Telnet access is enabled by default. Any changes to the enabled state of the Telnet server are retained through system restarts and power cycles.

Ethernet Connection Loss

If the Ethernet cable is disconnected from the director or switch during a Telnet session, one of three scenarios is possible:

- Replace the Ethernet cable before the client connection times out, and the Telnet session will continue.
- Wait 15 minutes until the client connection times out; then replace the Ethernet cable and restart the connection.
- If the client connection has already timed out, replace the Ethernet cable. Open a GUI-based or web-based interface SAN-management window. Toggle the enabled state of the CLI, thereby clearing the client connection. Restart the client connection.

Once the client connection is reestablished, verify your configuration's completeness and accuracy.

Backup and Restoration

A standalone Configuration Backup and Restore (CBR) utility is available for customers that do not use EFCM for backing up and restoring user configuration data. You can use this utility to backup and restore configuration data from all switch and director products running E/OS versions 4.0 and higher. The CBR utility is available for no charge in the Technical Documents section of the McDATA website at www.mcddata.com or by contacting your sales representative or service provider

The procedures for system backup and restoration are documented in the *Configuration Backup and Restore Utility Installation and User Guide* (958-000370), which is also available at www.mcddata.com.

This chapter describes the Command Line Interface (CLI) commands, including their syntax, purpose, and parameters, as well as examples of their usage and any output that they generate.

- *Command Overview* 2-2
- *New and Changed Commands* 2-2
- *config*..... 2-5
- *maint*..... 2-95
- *perf*..... 2-99
- *show* 2-138

Command Overview

Most of the commands in this chapter are listed in alphabetical order to make them easy to locate. Although the commands can be entered in any order, depending on the results desired (so long as the tree structure is followed), the order used herein for the zoning commands follows a typical order of entry. The various show commands are usually entered at the end of a group of other commands to verify configuration changes.

New and Changed Commands

The following CLI commands are new for this edition of the *Enterprise Operating System Command Line Interface User Manual*:

- [*config.fencing.addPolicy*](#) on page 2-10
- [*config.fencing.addPort*](#) on page 2-10
- [*config.fencing.deletePolicy*](#) on page 2-11
- [*config.fencing.removePort*](#) on page 2-12
- [*config.fencing.setParams*](#) on page 2-12
- [*config.fencing.setState*](#) on page 2-14
- [*config.fencing.show*](#) on page 2-14
- [*config.fencing.showTypeTable*](#) on page 2-16
- [*config.ficonCUPZoning.addControlHost*](#) on page 2-16
- [*config.ficonCUPZoning.deleteControlHost*](#) on page 2-17
- [*config.ficonCUPZoning.setState*](#) on page 2-17
- [*config.ficonCUPZoning.show*](#) on page 2-18
- [*config.ficonMS.setMIHPTO*](#) on page 2-18
- [*config.ficonMS.show*](#) on page 2-20
- [*config.ip.lineSpeed*](#) on page 2-21
- [*config.NPIV.maxPortIDs*](#) on page 2-22
- [*config.NPIV.maxPortIDs*](#) on page 2-22
- [*config.NPIV.setState*](#) on page 2-23

- [*config.NPIV.show*](#) on page 2-23
- [*config.port.rxCredits*](#) on page 2-26
- [*config.port.show*](#) on page 2-27
- [*config.port.showPortAddr*](#) on page 2-28
- [*config.port.swapPortByAddr*](#) on page 2-30
- [*config.port.swapPortByNum*](#) on page 2-30
- [*config.security.authentication.interface.api.outgoing*](#) on page 2-33
- [*config.security.authentication.interface.api.sequence*](#) on page 2-33
- [*config.security.authentication.interface.cli.sequence*](#) on page 2-34
- [*config.security.authentication.interface.eport.outgoing*](#) on page 2-34
- [*config.security.authentication.interface.eport.sequence*](#) on page 2-35
- [*config.security.authentication.interface.nport.outgoing*](#) on page 2-36
- [*config.security.authentication.interface.nport.sequence*](#) on page 2-36
- [*config.security.authentication.interface.osms.setKey*](#) on page 2-38
- [*config.security.authentication.interface.osms.outgoing*](#) on page 2-37
- [*config.security.authentication.interface.serial.enhancedAuth*](#) on page 2-38
- [*config.security.authentication.interface.show*](#) on page 2-39
- [*config.security.authentication.interface.web.sequence*](#) on page 2-39
- [*config.security.authentication.port.override*](#) on page 2-40
- [*config.security.authentication.port.show*](#) on page 2-41
- [*config.security.authentication.RADIUS.deadtime*](#) on page 2-42
- [*config.security.authentication.RADIUS.deleteServer*](#) on page 2-43
- [*config.security.authentication.RADIUS.attempts*](#) on page 2-42
- [*config.security.authentication.RADIUS.server*](#) on page 2-43
- [*config.security.authentication.RADIUS.show*](#) on page 2-44
- [*config.security.authentication.RADIUS.timeout*](#) on page 2-45
- [*config.security.authentication.switch.setSecret*](#) on page 2-45
- [*config.security.authentication.user*](#) on page 2-46

- [*config.security.authentication.user.add*](#) on page 2-46
- [*config.security.authentication.user.delete*](#) on page 2-47
- [*config.security.authentication.user.modify*](#) on page 2-48
- [*config.security.authentication.user.role*](#) on page 2-49
- [*config.security.authentication.user.show*](#) on page 2-50
- [*config.security.switchAcl.addRange*](#) on page 2-62
- [*config.security.switchAcl.deleteRange*](#) on page 2-63
- [*config.security.switchAcl.setState*](#) on page 2-63
- [*config.security.switchAcl.show*](#) on page 2-64
- [*config.security.ssh.resetKeys*](#) on page 2-61
- [*config.security.ssh.setState*](#) on page 2-61
- [*config.security.ssh.show*](#) on page 2-61
- [*config.switch.zoneFlexPars*](#) on page 2-80
- [*perf.thresholdAlerts.show*](#) on page 2-127
- [*show.auditLog*](#) on page 2-139
- [*show.epFrameLog.config*](#) on page 2-140
- [*show.epFrameLog.filterClassFFrames*](#) on page 2-140
- [*show.epFrameLog.noWrap*](#) on page 2-142
- [*show.epFrameLog.wrap*](#) on page 2-143
- [*show.fabric.principal*](#) on page 2-148
- [*show.fabric.topology*](#) on page 2-149
- [*show.fabricLog.noWrap*](#) on page 2-145
- [*show.fabricLog.wrap*](#) on page 2-146
- [*show.fencing.policies*](#) on page 2-150
- [*show.ficonCUPZoning*](#) on page 2-152
- [*show.ficonMS*](#) on page 2-152
- [*show.NPIV.config*](#) on page 2-159
- [*show.openSysMS.config*](#) on page 2-160
- [*show.port.opticeDD*](#) on page 2-169

- [show.port.opticInfo](#) on page 2-170
- [show.port.profile](#) on page 2-171
- [show.port.showPortAddr](#) on page 2-173
- [show.security.log](#) on page 2-181
- [show.security.switchAcl](#) on page 2-183

config

The config branch of the CLI command tree contains commands that set parameter values on the switch or director. These values are not temporary (session) values, but are retained across power cycles.

The commands in the config branch can only be accessed by a user with administrator level user rights.

CLI commands are activated on the switch immediately, except as noted.

In general, the config naming commands (except for the config.zoning commands) use the USASCII character set. All of the characters in this 128-character set (the first 7-bit subset of the ISO-8859-1 Latin-1 character set) are valid. Any exceptions are noted in the specific command descriptions.

config.enterpriseFabMode.setState

Syntax `setState enterpriseFabModeState`

Purpose This command sets the Enterprise Fabric Mode state for the fabric. The SANtegrity™ feature key must be installed to activate the Enterprise Fabric Mode state.

NOTE: The command [config.features.enterpriseFabMode](#) on page 2-6 has functionality that is identical to this command.

Parameters This command has one parameter.

enterpriseFabModeState	Specifies whether enterpriseFabMode is active. Valid values are <i>activate</i> and <i>deactivate</i> . Boolean 1 and 0 may be substituted as values.
------------------------	---

Command Example

```
Root> config enterpriseFabMode setState 1
```

NOTE: You cannot activate Enterprise Fabric Mode while Open Trunking is enabled.

config.features.enterpriseFabMode**Syntax**

```
enterpriseFabMode enterpriseFabModeState
```

Purpose

This command sets the Enterprise Fabric Mode state for the fabric. The SANtegrity™ feature key must be installed to activate the Enterprise Fabric Mode state.

Parameters

This command has one parameter.

`enterpriseFabModeState` Specifies whether `enterpriseFabMode` is active. Valid values are *activate* and *deactivate*. Boolean 1 and 0 may be substituted as values.

Command Example

```
Root> config features enterpriseFabMode 1
```

NOTE: The command [config.enterpriseFabMode.setState](#) on page 2-5 has functionality that is identical to this command.

config.features.ficonMS**Syntax**

```
ficonMS ficonMSState
```

Purpose

This command sets the enabled state of the FICON Management Server. The FICON Management Server feature key must be installed in order to enable the FICON Management Server State. (The Sphereon 4300 and Sphereon 4500 switches do not accept this command.)

NOTE: This command is displayed on a Sphereon 3016 and 3216 only if the feature key is installed.

NOTE: If the FICON Management Server is enabled, the default management style is the FICON Management Style. The Open Systems Management Style cannot be used.

Parameters This command has one parameter.

ficonMSState	Specifies whether the FICON Management Server is enabled. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.
--------------	---

Command Example **Root>** config features ficonMS 1

NOTE: The command [config.ficonMS.setState](#) on page 2-19 has functionality that is identical to this command.

config.features.installKey

Syntax installKey featureKey

Purpose This command allows the user to install a feature set that is enabled by the provided feature key. The switch can be either offline or online when this command is executed.

NOTE: If any currently installed features are being removed by the new feature key, the switch must be offline when the command is given.

Parameters This command has one parameter.

featureKey	Specifies the key you have received to enable optional software feature on a specific product. A feature key is a string of case-sensitive, alphanumeric ASCII characters. The number of characters may vary in the format; however, the key must be entered exactly, including the hyphens. An example of a feature key format is XxXx-XXxX-xxXX-xX.
------------	--

Command Example **Root>** config features installKey AaBb-CCdD-eeFF-gH

config.features.NPIV

Syntax `setState NPIVState`

Purpose This command sets the enabled state of the NPIV feature. The NPIV feature key must be installed in order to enable this feature.

Parameters This command has one parameter.

 NPIVState Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command Example **Root>** `config features NPIV enable`

NOTE: The command [config.NPIV.setState](#) on page 2-23 has functionality that is identical to this command.

config.features.openSysMS

Syntax `openSysMS openSysMSState`

Purpose This command sets the enabled state of the Open Systems Management Server (OSMS). OSMS is a feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device.

Parameters This command has one parameter.

 osmsState Specifies whether the Open Systems Management Server is enabled. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command Example **Root>** `config features openSysMS 1`

NOTE: The command [config.openSysMS.setState](#) on page 2-24 has functionality that is identical to this command.

config.features.openTrunking

Syntax `openTrunking openTrunkingState`

Purpose This command sets the enabled state of the OpenTrunking feature. The OpenTrunking feature key must be installed in order to enable open trunking.

Parameters This command has one parameter.

openTrunkingState This parameter can be set to *enable* or *disable* the OpenTrunking feature. Boolean 1 and 0 may be substituted as values.

Command Example **Root>** config features openTrunking 1

NOTE: The command [perf.openTrunking.setState](#) on page 2-107 has functionality that is identical to this command.

config.features.show

Syntax show

Purpose This command shows the product feature information configured for this switch.

Parameters This command has no parameters.

Command Example **Root>** config features show

Output The product feature data is displayed as a table that includes the following properties.

Installed Feature Set The feature set installed using a feature key. Only installed keys are displayed.

Feature Individual features within each set. In many cases, there is only one feature within each feature set.

State The state of the individual feature. Fabric-wide features are displayed as *Active/Inactive*. Features related to the switch are displayed as *Enabled/Disabled*.

Output Example

The output from the `config.features.show` command displays as follows.

Installed Feature Set	Feature	State
-----	-----	-----
Flex Ports	8 Flex Ports	Enabled
SANtegrity	Fabric Binding	Active
SANtegrity	Switch Binding	Enabled
SANtegrity	Enterprise Fabrics	Active
Open Trunking	Open Trunking	Enabled

NOTE: The command [show features](#) on page 2-150 has functionality that is identical to this command.

config.fencing.addPolicy

Syntax `addPolicy name`

Purpose This command configures a new fencing policy and assigns it a name. The new policy is assigned default settings, which must be changed before the policy is activated.

See [config.fencing.setParams](#) on page 2-12 for default settings.

Parameters This command has one parameter.

name	Specifies the name of the new fencing policy. This name can consist of any printable USASCII characters up to a maximum length of 63 characters. This name is case-sensitive.
------	---

Command Example

Root> `config fencing addPolicy Policy2`

NOTE: The maximum number of policies supported is 14.

config.fencing.addPort

Syntax `addPort name portNumber`

Purpose This command adds a port to the specified fencing policy.

Parameters This command has two parameters.

name	The name of the fencing policy.
portNumber	The new port number to add to the fencing policy, or <i>all</i> , which will add all of the individual ports to the fencing policy. Valid values for the port number are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

NOTE: A range of ports is not accepted as a valid input to this command (e.g., “0-29” is not acceptable).

The port values can also be substituted with one of the following keywords that will remove all the ports from the alert, and then use a specific type of port instead of individual port numbers.

Valid values are:

- eport - This will add all active E ports

NOTE: A fencing policy is not allowed to contain both port types and individual ports.

Command Example

```
Root> config fencing addPort 24
Root> config fencing addPort eport
```

config.fencing.deletePolicy

Syntax deletePolicy name

Purpose This command deletes a specified fencing policy. Only disabled fencing policies can be deleted.

Parameters	This command has one parameter.	
	name	The name of the fencing policy. You can also enter <i>all</i> for this argument. This will delete all of the configured fencing policies.

Command Example **Root>** config fencing deletePolicy Policy1

config.fencing.removePort

Syntax	removePort name portNumber	
Purpose	This command removes a port from the specified fencing policy.	
Parameters	This command has two parameters.	
	name	The name of the fencing policy.
	portNumber	The new port number to remove from the fencing policy, or <i>all</i> , which will remove all of the individual ports from the fencing policy. 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command Example **Root>** config fencing removePort 24

config.fencing.setParams

Syntax	setParams name typeNumber limit period
Purpose	This command sets the type, limit and period values for a specified fencing policy.

Parameters

This command has four parameters.

- name

The name of the fencing policy.
- typeName

This must be entered as a number that corresponds to an entry in the table shown below.
- limit

The count of fencing violations that must occur within the specified period in order for a port to be automatically disabled. Acceptable values are in the range of 1-255.

You may also enter *default* for this argument, which will set the default limit value for this fencing policy type.
- period

The number of seconds in which the violation count must equal or exceed the threshold limit in order for a port to be fenced.

You may also enter *default* for this argument, which will set the default period for this fencing policy type.

NOTE: The interval value is a fixed length amount of time. This interval is not a rolling window interval.

Type Number	Policy Type	Default Limit Value	Default Period Value
1	Protocol Errors	5	300 seconds

Type Number	Policy Type	Limit Value Range	Period Value Range
1	Protocol Errors	1 - 255	60 - 1800 seconds

Command Example

The meaning for each of these inputs can best be described using the following example sentence:

If ports 0,1, or 2 have more than 5 protocol errors on a single port within a period of 30 minutes, disable the offending port.

Where:

Port list	= 0, 1, 2
Fencing Type	= Protocol Errors
Limit	= 5
Period	= 1800 seconds

config.fencing.setState**Syntax**

`setState name enabledState`

Purpose

This command sets the enabled state of the specified fencing policy. A policy cannot be activated if it contains ports that are already controlled by a different fencing policy of the same type.

Parameters

This command has two parameters.

name	The name of the fencing policy.
enabledState	Sets the fencing policy enabled state. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 values may also be substituted.

Command Example

Root> `config fencing setState enable`

config.fencing.show**Syntax**

`show [name]`

Purpose

This command displays the settings for fencing policies.

Parameters This command has one optional parameter.

name The name of the fencing policy.

When no parameters are specified, the command will display the name, type, and state of all policies. If you use the optional parameter, it will display all the information about the policy.

NOTE: When the *name* parameter isn't supplied, then only 50 characters of the names of the policies will be displayed. You will have to enable Comma Delimited Mode to view the full name.

Command Example

```
Root> config fencing show
Root> config fencing show Policy_1
```

Output If you do not specify the *name* parameter, then the output shows the following information.

Name	The name of the policy. This will be concatenated to 50 characters in the summary display. The policy full name will be shown in comma delim mode.
Ports	The ports to which the fencing policy will be applied
Type	The type of the fencing policy.
Limit	The number of offenses that are allowed before a port is disabled.
Period	The amount of time that limit of number of offenses must exceed before a port is fenced.
State	The enabled state of the fencing policy.

Output Example The output from the config.fencing.show command displays as follows:

Name	Type	State
-----	-----	-----
Default Protocol Error Policy	Protocol Error	Disabled
Policy_1	Protocol Error	Disabled

The output from the `config.fencing.show Policy_1` command displays as follows:

```
Name:      Policy_1
Ports:     E ports
Type:      Protocol Error
Limit:     5
Period:    300 seconds
State:     Disabled
```

config.fencing.showTypeTable

Syntax `showTypeTable`

Purpose This command displays the table of different fencing types that can be assigned to a policy. This table is used for reference only.

Parameters This command has no parameters.

Command Example **Root>** `config fencing showTypeTable`

Output Example The output from the `config.fencing.showTypeTable` command displays as follows:

```
Number      Fencing Policy Types
-----
1           Protocol Errors
```

config.ficonCUPZoning.addControlHost

Syntax `addControlHost hostNodeWwn`

Purpose This command adds a control host to the Control Host List used to determine the FICON host(s) capable of viewing all ports. This list overrides the FCZ port visibility mask. The maximum entries in this list is 8.

Parameters This command has one parameter:

<code>hostNodeWwn</code>	The node WWN of the desired control host, entered in colon-delimited notation (e.g., 01:02:03:04:05:06:07:08)
--------------------------	---

Command Example **Root>** config ficonCUPZoning addControlHost 01:02:03:04:05:06:07:08

config.ficonCUPZoning.deleteControlHost

Syntax deleteControlHost hostNodeWwn

Purpose This command removes one or all control hosts from the Control Host List used to determine the FICON host(s) capable of viewing all ports. This list overrides the FCZ port visibility mask.

Parameters This command has one parameter:

hostNodeWwn	The node WWN of the desired control host, entered in colon-delimited notation (e.g., 01:02:03:04:05:06:07:08). You can also enter <i>all</i> to remove the entire list, if no attached hosts have supervisory privileges.
-------------	---

Command Example **Root>** config ficonCUPZoning deleteControlHost all

config.ficonCUPZoning.setState

Syntax setState ficonCUPZoningState

Purpose This command sets the enabled state of FICON CUP Zoning. The FICON Management Server feature key must be installed in order to enable the FICON CUP Zoning State. (The Sphereon 4300 and Sphereon 4500 switches do not accept this command.)

NOTE: If the FICON Management Server is enabled, the default management style is the FICON Management Style. The Open Systems Management Style cannot be used.

Parameters This command has one parameter.

ficonCUPZoningState	Specifies whether the FICON Management Server is enabled. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.
---------------------	---

Command Example **Root>** config ficonCUPZoning setState 1

config.ficonCUPZoning.show

Syntax show

Purpose This command displays the contents of the host control list and the enabled state of FICON CUP Zoning.

Parameters This command has no parameters.

Command Example **Root>** config ficonCUPZoning show

Output The data is displayed as a table that includes the following information:

FICON CUP Zoning State	The enabled state of the FICON CUP Zoning feature
Host Control List	List of 0-8 control hosts, displays "empty" for control host list with no members.

Output Example The output from the config ficonCUPZoning show command displays as follows:

FICON CUP Zoning State: Enabled

Host Control List

 01:02:03:04:05:06:07:08
 09:0A:0B:0C:0D:0E:0F:00

NOTE: The command [show.ficonCUPZoning](#) on page 2-152 has functionality that is identical to this command.

config.ficonMS.setMIHPTO

Synopsis setMIHPTO timeout

Purpose This command sets the Ficon MS MIHPTO value in seconds. The default value is 180 seconds (3 minutes).

Parameters This command has one parameter.

timeout	Valid values are 15, 30, 45, 60, 120, 180, 240, 300, 360, 420, 480, 540, and 600.
---------	---

Command Example `Root> config ficonms setMIHPTO 180`

config.ficonMS.setState

Syntax `setState ficonMSState`

Purpose This command sets the enabled state of the FICON Management Server. The FICON Management Server feature key must be installed in order to enable the FICON Management Server State. (The Sphereon 4300 and Sphereon 4500 switches do not accept this command.)

NOTE: This command is displayed on a Sphereon 3016 only if the feature key is installed.

NOTE: If the FICON Management Server is enabled, the default management style is the FICON Management Style. The Open Systems Management Style cannot be used.

Parameters This command has one parameter.

ficonMSState	Specifies whether the FICON Management Server is enabled. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.
--------------	---

Command Example `Root> config ficonMS setState 1`

NOTE: The command [config.features.ficonMS](#) on page 2-6 has functionality that is identical to this command.

config.ficonMS.show

Syntax `show`

Purpose This command shows the Ficon MS settings

Parameters This command has no parameters.

Command Example **Root>** `config ficonMS show`

Output The data is displayed as a table that includes the following information:

Ficon MS State	The state of the FICON MS feature.
Ficon MIHPTO	The FICON MIHPTO value in seconds.

Output Example The output from the config ficonMS show command displays as follows:

```
Ficon MS State: Disabled
Ficon MIHPTO (seconds): 180
```

config.ip.ethernet

Syntax `ethernet ipAddress gatewayAddress subnetMask`

Purpose This command sets the Ethernet network settings.

ATTENTION! The Telnet connection can be lost when these Ethernet network settings are changed.

NOTE: If the IP address is reconfigured, your Telnet client must be reconnected to the new IP address. A new login will be requested.

Parameters	This command has three parameters.	
	ipAddress	Specifies the new IP address for the director or switch. The address must be entered in dotted decimal format (for example, 10.0.0.0).
	gatewayAddress	Specifies the new gateway address for the Ethernet interface. The address must be entered in dotted decimal format (for example, 0.0.0.0).
	subnetMask	Specifies the new subnet mask for the Ethernet interface. The address must be entered in dotted decimal format (for example, 255.0.0.0).

Command Example **Root>** config ip ethernet 10.0.0.0 0.0.0.0 255.0.0.0

config.ip.lineSpeed

Synopsis	lineSpeed speed duplex	
Purpose	This command sets the Ethernet line speed	
Parameters	This command has two parameters. One of the parameters is optional depending on the combination.	
	speed	The line speed. Options are auto, 10, or 100. If auto is entered then the optional <i>duplex</i> should not be entered.
	duplex	The duplex mode for the connection. Options are <i>full</i> or <i>half</i> .

Command Example **Root>** config ip lineSpeed 10 half

config.ip.show

Syntax	show
Purpose	This command shows the LAN configuration.
Parameters	This command has no parameters.

Command Example **Root>** config ip show

Output The LAN configuration data is displayed as a table that includes the following properties.

IP Address	The IP address.
Gateway Address	The gateway address.
Subnet Mask	The subnet mask.

Output Example The output from the config.ip.show command displays as follows.

```
IP Address:      10.0.0.0
Gateway Address: 0.0.0.0
Subnet Mask:     255.0.0.0
```

config.NPIV.maxPortIDs

Syntax maxPortIDs portNumber maxIDs

Purpose This command configures the maximum number of NPIV logins that are allowed on the specified port.

Parameters This command has two parameters.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 all - applies the maxIDs parameter value to every port on the product
maxIDs	Specifies the maximum number of NPIV logins allowed on the specified port. Valid values are in the range 1-256.

Command Example **Root>** config NPIV maxPortIDs 128

Root> config NPIV portNumber 60

config.NPIV.setState

Syntax `setState NPIVEnabledState`

Purpose This command sets enabled state of the NPIV feature. The NPIV feature key must be installed in order to enable this feature.

Parameters This command has one parameter.

 NPIVEnabledState This parameter can be set to *enable* or *disable*. Boolean 1 and 0 values may also be substituted.

Command Example **Root>** `config NPIV setState enable`

config.NPIV.show

Syntax `show`

Purpose This command displays the current NPIV configuration for all ports.

Parameters This command has no parameters.

Command Example **Root>** `config NPIV show`

Output This command displays the following NPIV configuration data:

 NPIV state The current enabled/disabled state of the NPIV feature.

 Max Allowed NPIV Login Table. A table mapping each port number on the switch to a corresponding max number of NPIV logins setting.

Output Example The output from the config.NPIV.show command displays as follows:

```
NPIV state: Enabled
Port          Max Allowed NPIV Logins
-----
1             10
2             10
3             10
4             0
5             0
```

```
6      130
...

```

NOTE: The command [show.NPIV.config](#) on page 2-159 has functionality that is the same as this command.

config.openSysMS.setHostCtrlState

Syntax `setHostCtrlState HostContrlState`

Purpose This command sets the enabled state of the Open Systems Management Server Host Control.

Parameters This command has one parameter:

HostContrlState	This parameter can be set to <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
-----------------	--

Command Example **Root>** `config openSysMS setHostCtrlState enable`

config.openSysMS.setState

Syntax `setState osmsState`

Purpose This command sets the enabled state of the Open Systems Management Server (OSMS). OSMS is a feature that allows host control and inband management of the director or switch through a management application that resides on an open-systems interconnection (OSI) device.

Parameters This command has one parameter.

osmsState	Specifies whether the Open Systems Management Server is enabled. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.
-----------	--

Command Example **Root>** `config openSysMS setState 1`

NOTE: The command [config.features.openSysMS](#) on page 2-8 has functionality that is identical to this command.

config.port.blocked

Syntax `blocked portNumber blockedState`

Purpose This command sets the blocked state for a port.

Parameters This command has two required parameters.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
blockedState	Specifies the blocked state for the port. Valid values are <i>true</i> and <i>false</i> . Boolean 1 and 0 may be substituted as values.

Command Examples

Root> `config port blocked 4 false`

Root> `config port blocked 4 0`

config.port.fan

Syntax `fan portNumber fanOn`

Purpose This command sets the fabric address notification (FAN) state for a port (Sphereon 4300 and Sphereon 4500 switches only). This configuration can be applied to any port regardless of its current configuration. The FAN value is applied at the time the port is configured and operated in a loop.

Parameters	This command has two required parameters.	
	portNumber	Specifies the port number. Valid values are: 0–23 for the Sphereon 4500
	fanOn	Specifies the FAN state for the port. Valid values are <i>true</i> and <i>false</i> . Boolean 1 and 0 may be substituted as values.

Command Example **Root>** config port fan 4 1

config.port.name

Syntax	name portNumber portName	
Purpose	This command sets the name for a port.	
Parameters	This command has two required parameters.	
	portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
	portName	Specifies the name for the port. The port name must not exceed 24 characters in length.

Command Example **Root>** config port name 4 Sam's tape drive

config.port.rxCredits

Syntax	rxCredits portNumber numRxCredits	
Purpose	This command is used to set the number of initial BB Credits for a given port. The number of credits assigned must fall between the minimum and maximum allowed values for the port.	

Parameters	This command has two required parameters:
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
numBBCredits	Specifies the number of Rx BB Credits to assign the specified port. For the Sphereon 4300 and Sphereon 4500 the RxCredits per port must be between 2 and 12. The total number of Rx Credits assigned across all ports must not exceed the maximum pool size of 150. For the Intrepid family, the RxCredits per FPM/UPM port must be between 1 and 60. The RxCredits per XPM port must be between 4 and 400. There is no pool limitation.

Command Example **Root>** config port rxCredits 8 40

config.port.show

Syntax	show portNumber
Purpose	This command displays the current configuration for the specified port.
Parameters	This command has one parameter.
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command Example**Root>** config port show 4**Output**

This command displays as a table that includes the following properties.

Port Number	The port number.
Name	The configured port name.
Blocked	The blocked state. Valid values are <i>true</i> and <i>false</i> .
FAN	The fabric address notification (FAN) state. Valid values are <i>true</i> and <i>false</i> . (Sphereon 4300 and Sphereon 4500 switches only.)
Type	The port type. Valid values are: <ul style="list-style-type: none"> • <i>F Port</i> • <i>E Port</i> • <i>G Port</i> • <i>Fx Port</i> (Sphereon 4300 and Sphereon 4500 only) • <i>Gx Port</i> (Sphereon 4300 and Sphereon 4500 only)
Speed	The port speed. Valid values are <i>1 Gb/sec</i> , <i>2 Gb/sec</i> , and <i>Negotiate</i> .
Rx BB Credits	The number of configured Rx BB Credits.

Output Example

The output from the config.port.show command displays as follows.

```
Port Number:      4
Name:             Sam's tape drive
Blocked:          false
Type:             F Port
Speed:            2 Gb/sec
Rx BB Credits:    12
```

config.port.showPortAddr**Syntax**

showPortAddr

Purpose

This command displays the port address configuration for all ports.

NOTE: The command [show.port.showPortAddr](#) on page 2-173 has functionality that is the same as this command.

Parameters This command has no parameters.

Command Example `Root> config port showPortAddr`

Output The port configuration is shown as a table of properties. The following properties are displayed:

Port	The port number
Original Addr	The original port address of the port
Current Addr	The current port address of the port
Swapped Port Num	If the port is swapped with another port, it will show the port number of the port it is swapped with.

Output Example

Port	Original Addr	Current Addr	SwappedPort Num
----	-----	-----	-----
0	4	4	
1	5	5	
2	6	7	3
3	7	6	2
4	8	8	
5	9	9	
6	a	a	
7	b	b	
8	c	c	
...			

config.port.speed

Syntax `speed portNumber portSpeed`

Purpose This command sets the speed for a port. A port can be configured to operate at 1 Gb/sec, 2 Gb/sec, or a negotiated speed. The port speed can be set only to 1 Gb/sec if the switch speed is 1 Gb/sec. An attempt to set the port speed to 2 Gb/sec or to negotiate in a switch with a 1 Gb/sec switch speed results in an error message.

If the port speed is set to *negotiate*, the port and the device to which it is attached negotiate the data speed setting to either 1 Gb/sec or 2 Gb/sec.

ATTENTION! Port speed changes temporarily disrupt port data transfers.

Parameters

This command has two required parameters.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portSpeed	Specifies the speed of the port. Valid values are <i>1g</i> , <i>2g</i> , and <i>negotiate</i> .

Command Examples

```
Root> config port speed 4 2g
```

```
Root> config port speed 6 negotiate
```

config.port.swapPortByAddr**Syntax**

```
swapPortByAddr portAddr1 portAddr2
```

Purpose

This command will swap two ports given the port addresses. The ports must be offline to perform this operation.

Parameters

This command has two required parameters:

portAddr1	Port address, in hexadecimal format, of the desired port to be swapped
portAddr2	Port address, in hexadecimal format, of the desired port to be swapped

Command Example

```
Root> config port swapPortByAddr 1e 1f
```

config.port.swapPortByNum**Syntax**

```
swapPortByNum portNum1 portNum2
```

Purpose This command will swap two ports given the port numbers. The ports must be offline to perform this operation.

Parameters This command has two required parameters:

portNum1	Port number, in hexadecimal format, of the desired port to be swapped
portNum2	Port number, in hexadecimal format, of the desired port to be swapped

Command Example **Root>** config port swapPortByAddr 1e 1f

config.port.type

Syntax type portNumber portType

Purpose This command sets the allowed type for a port.

A port can be configured as an F_Port, an E_Port, or a G_Port. On a Sphereon 4300 or Sphereon 4500, a port can also be an Fx_port or Gx_port.

NOTE: On the Sphereon 4300 Switch, the E_Port, G_Port, and GX_Port options are not valid, unless the Fabric Capable feature is enabled. For more information, see the *McDATA Sphereon 4300 Switch Installation and Service Manual* (620-000171).

The port configurations function as follows:

- F_Port—cannot be used as an interswitch link, but may attach to a device with an N_Port.
- E_Port—only other switches may attach to this type of port.
- G_Port—either a device or another switch may attach to this type of port.
- Fx_Port — allows Arbitrated Loop operation in addition to the functionality of an F_Port. (Sphereon 4300 and Sphereon 4500 only.)
- Gx_Port—allows Arbitrated Loop operation in addition to the functionality of an F_Port or an E_Port. (Sphereon 4300 and Sphereon 4500 only.)

Parameters

This command has two required parameters.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portType	Specifies the type of the port. Valid values for the port type are: <i>eport</i> <i>fport</i> <i>gport</i> <i>fxport</i> (Sphereon 4300 and Sphereon 4500 only) <i>gxport</i> (Sphereon 4300 and Sphereon 4500 only)

Command Example

```
Root> config port type 4 fport
```

config.security

The security command on the configuration branch enters the security configuration branch. All commands under this branch operate on a particular security attribute.

Some security configuration commands (namely those under the fabricBinding branch) are different from other CLI commands in that they are not single action commands that take effect immediately. These commands implement a rudimentary membership list editor. A user works on a temporary copy of a membership list in the editor and can perform actions such as adding or deleting fabric members. The edited copy can then be activated to the fabric. It should be noted that not all verification of membership lists can be made in the pending copy. Therefore, it is possible that a user will build up a pending membership list definition without errors, but will encounter errors when saving to the fabric. It should also be noted that the state of the pending configuration must be set to 'restrict' in order to make any changes to the (pending) fabric membership list.

config.security.authentication.interface api.outgoing

Syntax outgoing enabledState

Purpose This command determines if outgoing CHAP authentication is used on all API sessions. If this is enabled, the switch will issue a CHAP challenge to authenticate all new API connections.

Parameters This command has one parameter:

enabledState	This parameter enables and disables outgoing CHAP authentication for API sessions. Valid values for this parameter are <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
--------------	--

Command Example **Root>** config security authentication interface api
 outgoing enable

config.security.authentication.interface api.sequence

Syntax sequence method1 [method2]

Purpose This command sets the sequence that the API interface will use to authenticate. When the preferred method cannot be contacted, the backup method will be used to authenticate the API session.

Parameters This command has one required parameter, and one optional parameter:

method1	This sets the preferred method of authentication. Accepted values are <i>local</i> or <i>RADIUS</i> .
method2	This optional parameter sets the backup method of authentication. This backup method is used when the preferred method cannot be contacted. Accepted value is <i>local</i> .

NOTE: A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command Example

```
Root> config security authentication interface api
sequence RADIUS local
```

config.security.authentication.interface.cli.sequence

Syntax sequence method1 [method2]

Purpose This command sets the sequence that the CLI interface will use to authenticate. When the preferred method cannot be contacted, the backup method will be used to authenticate the CLI login.

Parameters This command has one required parameter, and one optional parameter:

method1 This sets the preferred method of authentication for the CLI interface. Accepted values are *local* or *RADIUS*.

method2 This optional parameter sets the backup method of authentication for the CLI interface. This backup method is used when the preferred method cannot be contacted. Accepted value is *local*.

NOTE: A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command Example

```
Root> config security authentication interface cli
sequence RADIUS local
```

config.security.authentication.interface.eport.outgoing

Syntax outgoing enabledState

Purpose This command determines if outgoing CHAP authentication is used on E port connections. If this is enabled, the switch will issue a CHAP challenge to authenticate the remote end of the ISL.

NOTE: This command requires that the SANtegrity Authentication feature key be installed.

Parameters This command has one parameter:

enabledState	This parameter enables and disables outgoing CHAP authentication on all ISLs. Accepted values for this parameter are <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
--------------	--

Command Example **Root>** config security authentication interface eport
outgoing disable

config.security.authentication.interface.eport.sequence

Syntax sequence method1 [method2]

Purpose This command sets the sequence that the E port interface will use to authenticate. When the preferred method cannot be contacted, the backup method will be used to authenticate the remote end of the ISL.

NOTE: This command requires that the SANtegrity Authentication feature key be installed.

Parameters This command has one required parameter, and one optional parameter:

method1	This sets the preferred method of authentication. Accepted values are <i>local</i> or <i>RADIUS</i> .
method2	This optional parameter sets the backup method of authentication. This backup method is used when the preferred method cannot be contacted. Accepted value is <i>local</i> .

NOTE: A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command Example

```
Root> config security authentication interface eport
sequence RADIUS local
```

config.security.authentication.interface.nport.outgoing

Syntax outgoing enabledState

Purpose This command determines if outgoing CHAP authentication is used on N port connections. If this is enabled, the switch will issue a CHAP challenge to authenticate the remote device.

NOTE: This command requires that the SANtegrity Authentication feature key be installed.

Parameters This command has one parameter:

enabledState	This parameter enables and disables outgoing CHAP authentication on all ISLs. Accepted values for this parameter are <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
--------------	--

Command Example

```
Root> config security authentication interface eport
outgoing disable
```

config.security.authentication.interface.nport.sequence

Syntax sequence method1 [method2]

Purpose This command sets the sequence that the N_port interface will use to authenticate. When the preferred method cannot be contacted, the backup method will be used to authenticate the remote end of the ISL.

NOTE: This command requires that the SANtegrity Authentication feature key be installed.

Parameters This command has one required parameter, and one optional parameter:

method1	This sets the preferred method of authentication. Accepted values are <i>local</i> or <i>RADIUS</i> .
method2	This optional parameter sets the backup method of authentication. This backup method is used when the preferred method cannot be contacted. Accepted value is <i>local</i> .

NOTE: A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command Example

```
Root> config security authentication interface nport
sequence RADIUS local
```

config.security.authentication.interface.osms.outgoing

Syntax `outgoing enabledState`

Purpose This command determines if outgoing authentication is used on all OSMS requests. The OSMS key must be configured prior to setting the outgoing state to enabled.

NOTE: The SANtegrity Authentication feature key must be installed to configure the OSMS outgoing state.

Parameters This command has one parameter:

enabledState	This parameter enables and disables FCCT authentication. Accepted values for this parameter are <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
--------------	---

Command Example

```
Root> config security authentication interface osms
outgoing 1
```

config.security.authentication.interface.osms.setKey

Syntax `setKey`

Purpose This command sets the FCCT key that is associated to the single OSMS username. This username is a static entry in the local authentication database. This user is not viewable. This command effectively sets the key that will be used in all OSMS authenticated requests. This entry in the user database is only used for the OSMS interface, and cannot be changed.

After issuing this command, you are directed to a password prompt where the actual 16-byte key is entered. After entering the new secret, it must be confirmed in the following prompt. After confirmation, you will be returned to the initial prompt that the command was executed from. No characters will be echoed back to the screen when entering a password, or when confirming a password.

NOTE: The SANtegrity Authentication feature key must be installed to configure the FCCT key.

Parameters This command has no required parameters.

Command Example `Root> config security authentication interface osms
setKey`

config.security.authentication.interface.serial.enhancedAuth

Syntax `enhancedAuth enhancedAuthState`

Purpose This command sets the enhanced serial authentication state. Enhanced Serial Authentication will require a user to enter a password when gaining access to the serial port interface.

Parameters This command has one parameter:

`enhancedAuthState` This parameter enables and disables enhanced authentication on the serial port interface. Accepted values for this parameter are *enable* or *disable*. Boolean 1 and 0 values may also be substituted.

Command Example **Root>** config security authentication serial enhancedAuth enable

config.security.authentication.interface.show

Syntax show interface

Purpose This command displays the settings in the local authentication database for a single interface.

NOTE: The SANtegrity Authentication feature key must be installed to view the eport and nport information, and the OSMS information.

Parameters This command has one parameter.

interface	The interface that will be displayed. Valid values for this parameter are:
	<i>cli</i>
	<i>web</i>
	<i>osms</i>
	<i>api</i>
	<i>serial</i>
	<i>eport</i>
	<i>nport</i> .

Command Example **Root>** config security authentication interface show Web

Output Example The output for the config.security.authentication.interface.show command displays as follows:

```
Interface: Web
Outgoing:  N/A
Incoming:  N/A
Sequence:  Local, RADIUS
```

config.security.authentication.interface.web.sequence

Syntax sequence method1 [method2]

Purpose This command sets the sequence that the Web interface will use to authenticate. When the preferred method cannot be contacted, the backup method will be used to authenticate the Web login.

Parameters This command has one required parameter, and one optional parameter:

method1	This sets the preferred method of authentication for the CLI interface. Accepted values are <i>local</i> or <i>RADIUS</i> .
method2	This optional parameter sets the backup method of authentication for the CLI interface. This backup method is used when the preferred method cannot be contacted. Accepted value is <i>local</i> .

NOTE: A preferred method of *local* and a backup method of *RADIUS* is not an accepted combination because the *local* method can always be contacted.

Command Example

```
Root> config security authentication interface cli
sequence RADIUS local
```

config.security.authentication.port.override

Syntax `override portNumber [overrideState]`

Purpose This command sets the outgoing override state for a single port. This setting allows you to override the default outgoing authentication state for either the E_port or N_port interface. The default setting will cause the port to use the outgoing state configure for the corresponding interface (either E_port or N_port).

NOTE: This command requires that the SANtegrity Authentication feature key be installed.

Parameters	This command has one required parameter, and one optional parameter:
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
overrideState	This parameter sets the outgoing authentication state for the specified port. Valid values are <i>enable</i> , <i>disable</i> , or <i>default</i> . Boolean 1 and 0 values may also be substituted.

Command Example **Root>** config security authentication port override 138 enable

config.security.authentication.port.show

Syntax	show				
Purpose	This command displays a table displaying the outgoing override state for each port.				
Parameters	This command has no parameters.				
Command Example	Root> config security authentication port show				
Output	This command displays all valid user names in the local database for the specified interface.				
	<table> <tr> <td>Port</td><td>The port number.</td></tr> <tr> <td>Override State</td><td>The outgoing authentication override state.</td></tr> </table>	Port	The port number.	Override State	The outgoing authentication override state.
Port	The port number.				
Override State	The outgoing authentication override state.				
Output Example	The output for the config.security.authentication.port.show command displays as follows:				

Port	Override State
----	-----
0	Default
1	Default
2	Enable
3	Default
4	Disable

config.security.authentication.RADIUS.attempts

syntax attempts index attempts

Purpose This command configures the number of attempts a packet will be sent to a RADIUS server if a response is not received before the timeout. After the transmit attempt limit is reached, the switch will, if applicable, move on to the next defined RADIUS server. The default is 3 attempts.

Parameters This command has two required parameters:

index	Index of the RADIUS sever (1-3) to change the transmit attempts value.
attempts	The number of transmit attempts. Valid values are between 1 and 100.

Command Example **Root>** config security authentication RADIUS attempts 3 20

config.security.authentication.RADIUS.deadtime

Syntax deadtime minutes

Purpose This command configures the number of minutes a RADIUS server is marked as “dead”. If a RADIUS server does not respond to an authentication request, it can be marked as “dead” for a specified time interval. This may speed up authentication by eliminating timeouts and retransmissions. If no alternate RADIUS servers are available (when only one server is configured or when all are marked dead), then the deadtime is ignored. Deadtime may be 0 to 1440 minutes. The default is 0.

Parameters	This command has one required parameter:	
	minutes	The number of minutes a RADIUS server is marked “dead” before it is contacted again. Valid values are between 0 and 1440.

Command Example **Root>** config security authentication RADIUS deadtime 120

config.security.authentication.RADIUS.deleteServer

Syntax	deleteServer index	
Purpose	This command removes a RADIUS server from the RADIUS server list. If you delete a server, and there are servers configured in higher numbered slots, these servers will be automatically moved up to the first available slots.	
Parameters	This command has one required parameter.	
	index	Index of the server to be removed.

Command Example **Root>** config security authentication RADIUS deleteServer
3

config.security.authentication.RADIUS.server

Syntax	server index [IP:port]
Purpose	This command adds or modifies one RADIUS server, at a given index, that will be used for authentication. Servers are queried in the order listed, so the primary server must be the first one in the list.
	There are three slots available for RADIUS servers. Servers will be added into the list by the index value. The range is 1 to 3. If a server is added and there is an empty slot before that server, it will be shifted up to the empty slot. The IP:port is the IP address and the UDP port on the RADIUS server.

NOTE: If you want to configure a RADIUS server without a key, you must specify the key as "". The set of double quotes is an empty string in the CLI.

Parameters This command has one required parameter, and two optional parameters:

index	Index of the RADIUS server (1-3) to add/modify.
IP	IP address of the server.
port	The UDP port number.

Command Example **Root>** config security authentication RADIUS server 3 14.2.114.183:6

config.security.authentication.RADIUS.show

Syntax show

Purpose This command displays the current RADIUS server configuration.

Parameters This command has no parameters.

Command Example **Root>** config security authentication RADIUS show

Output This command displays all three configured RADIUS servers.

Deadtime	The amount of time a server is marked as “dead”.
Server	The IP address and UDP port of the configured RADIUS server.
Attempts	The number of transmit attempts.
Timeout	The timeout value for a server in seconds.

Output Example The output for the config.security.authentication.RADIUS.show command displays as follows:

Deadtime: 0

Index	IP Address	Port	Attempts	Timeout
----	-----	----	-----	-----
1	1.1.1.1	1111	3	2
2	2.2.2.2	2222	3	2
3				

config.security.authentication.RADIUS.timeout

Syntax timeout index seconds

Purpose This command configures the number of seconds to wait for a response from the RADIUS server before retransmitting a packet. The default is 2 seconds.

Parameters This command has two required parameters:

index	Index of the RADIUS sever (1-3) to change the timeout value.
seconds	The number of seconds before the RADIUS server retransmits. Valid values are between 1 and 1000.

Command Example **Root>** config security authentication RADIUS timeout 3 360

config.security.authentication.switch.setSecret

Syntax SetSecret

Purpose This command sets the CHAP secret that is associated with the switch. This command effectively sets the secret for the local WWN username in the local authentication user database. The switch secret is used for all incoming CHAP challenges on the E port and N port interfaces.

After issuing this command, you are directed to a “password” prompt where the actual 16-byte secret is entered. After entering the new secret, it must be confirmed in the following prompt. After confirmation, you are returned to the initial prompt that the command was executed from. No characters will be echoed back to the screen when entering a password, or when confirming a password. See [Passwords and Secrets](#) on page 1-14 for valid characters.

NOTE: The SANtegrity Authentication feature key must be installed to configure switch secret.

Parameters This command has no required parameters.

Command Example

```
Root> config security authentication switch setSecret
```

config.security.authentication.user

One of the fundamental concepts of the authentication portion of the Command Line Interface is that all secured interfaces have interchangeable users that are stored in a single local authentication user database. In the past, CLI has supported authorization for only two username/password pairs (one Administrator-level and another Operator-level). These two username/password pairs were also unique to CLI interface. With this release, a CLI user can now configure multiple users for his own interface, as well as for other management entities and FC connections. For this reason, the security.userrights branch of commands has been removed from the command tree.

config.security.authentication.user.add

Syntax `add username interface1 [interface2]`

Purpose This command adds a new user to the local authentication database. Each user can be assigned a combination of interfaces that will authenticate the new username/password combination. After executing this command, the user will be moved to a new password prompt where the user will enter a password; the password must then be confirmed in next prompt. After confirming the new password, the user will be returned to the initial prompt. No characters will be echoed back to the screen when entering a password, or when confirming a password.

All new users will be assigned a role of “none”; a subsequent “role” command must be executed to assign a role. Web and CLI users must be assigned a role before they can access the CLI or Web interfaces.

NOTE: The SANtegrity Authentication feature key must be installed to configure E port and N port usernames.

Parameters This command has two required parameters, and an additional password parameter at the prompt after the command.

username	The new user name that will be added to the local authentication database. If the entered user name already exists in the user database, an error will be shown. This parameter can be from 1-23 characters in length for an API, Web or CLI username. E Port and N Port usernames must be entered as a standard colon delimited WWN. All characters in the printable USASCII character set are valid with the exception of spaces, single quotes, and double quotes.
interfaces	This is a list of interfaces that will be assigned to the associated username. Accepted values for this parameter are: <i>cli</i> <i>web</i> <i>api</i> <i>eport</i> <i>nport</i>
password	Sets the password for the new login username. This parameter can be from 1-24 characters in length for a Web or CLI password. CHAP secrets and FCCT keys must be exactly 16 bytes long for API, OSMS, E Port, and N Port interfaces. This parameter will not be echoed to the screen. See Passwords and Secrets on page 1-14 for valid characters.

NOTE: Currently the only possible combination of multiple interfaces is (Web and CLI).

Command Example

```
Root> config security authentication user add
01:2A:3f:4:5:0:0 eport
```

config.security.authentication.user.delete

Syntax delete username

Purpose This command deletes an entry from the local authentication database. Both the Web and CLI interfaces must have at least one valid username with an “Administrator” role.

Parameters This command has one parameter:

username	A valid username in the local authentication database.
----------	--

Command Example **Root>** config security authentication user delete
01:2A:3f:4:5:0:0

config.security.authentication.user.modify

Syntax modify username interface1 [interface2]

Purpose This command modifies an existing user in the local authentication database. The user password and the combination of interfaces can be modified with this command. After executing this command, you are prompted to enter a password, similar to behavior of the user.add command.

The role of a user will remain the same unless the currently assigned role is invalid for the new combination of interfaces. If the role is no longer valid for an interface combination, the role will be changed back to “none”. At least one username with an “Administrator” role must exist in the user database at all times for both the Web and CLI interfaces.

NOTE: The SANtegrity Authentication feature key must be installed to configure E port and N port usernames.

Parameters This command has two required parameters, and an additional password parameter at the prompt after the command:

username	The existing user name whose fields will be modified in the local authentication database. If the entered user name does not exist in the user database, an error will be shown. This parameter can be from 1-23 characters in length for an API, Web or CLI username. E Port and N Port usernames must be entered as a standard colon delimited WWN. All characters in the printable USASCII character set are valid with the exception of spaces, single quotes, and double quotes.
interfaces	This is a list of interfaces that will be assigned to the associated username. Accepted values for this parameter are: <i>cli</i> <i>web</i> <i>api</i> <i>eport</i> <i>nport</i> .
password	Sets the password for the existing username. This parameter can be from 1-24 characters in length for a Web or CLI username. CHAP secrets must be exactly 16 bytes long for API, OSMS, E Port, and N Port interfaces. This parameter will not be echoed to the screen. See Passwords and Secrets on page 1-14 for valid characters.

NOTE: Currently the only possible combination of multiple interfaces is (Web and CLI) or (E port or N port).

Command Example

```
Root> config security authentication user modify
01:2A:3f:4:5:0:0 nport
```

config.security.authentication.user.role

Syntax role username privilegeLevel

Purpose This command sets the role value that is associated to an existing username. The role value can either be set to an administrator or an operator. This value defaults to “none” when the user is first added to the database. This value must be changed for all new CLI and Web users before they will be allowed access to their respective interfaces.

Parameters This command has two required parameters:

username	A valid Web or CLI username in the local authentication database.
privilegeLevel	This parameter assigns the privilege level to a username. Currently only Web and CLI users can be assigned a role value. This parameter must be either <i>administrator</i> or <i>operator</i> .

Command Example **Root>** config security authentication user role
01:2A:3f:4:5:0:0 administrator

config.security.authentication.user.show

Syntax show interface

Purpose This command displays a single interface from the local authentication database.

Parameters This command has one optional parameter:

interface	The interface that will be displayed. Accepted values for this parameter are: <i>cli</i> <i>web</i> <i>api</i> <i>eport</i> <i>nport</i> .
-----------	---

Command Example **Root>** config security authentication user show web

Output Example The output for the config.security.authentication.user.show command displays as follows:

Interface: Web

Username	Interfaces	Role
-----	-----	-----
johndoe_1223	Web, CLI	Administrator
ewsOperator	Web	Operator
Operator	Web, CLI	Operator

config.security.fabricBinding

Fabric Binding functionality, provided by the SANtegrity Binding feature, allows you to bind the switch or director to specified fabrics so that it can communicate only with those fabrics. With Fabric Binding enabled, the product can communicate only with fabrics that are included in the Fabric Binding Membership List (FBML).

Using Fabric Binding, you can allow specific switches to attach to specific fabrics in the SAN. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

Fabric Binding
Commands

The config.security.fabricBinding commands function in a different way from most CLI commands, which are single action commands that take effect immediately. Most of the Fabric Binding commands affect a temporary copy of an FBML in the work area, which is called the Pending FBML. When this temporary copy, the pending list, is activated to the fabric, it is called the Active FBML.

ATTENTION! One factor to consider, when using CLI commands to view and configure Fabric Binding settings, is that the SANpilot® interface can change Fabric Binding status and FBMLs, if it is used at the same time as the CLI.

Because not all the verification of the Pending FBML can occur on the temporary copy in the work area, it is possible, however unlikely, that the copy of the list encounters no errors until the list is activated to the fabric.

NOTE: A Sphereon 4300 Switch cannot participate in a fabric, unless the Fabric Capable feature is enabled. For more information, see the *McDATA Sphereon 4300 Switch Installation and Service Manual* (620-000171).

Fabric Binding
Membership
Terminology

Two types of FBMLs are configured using the CLI:

- **Active FBML:** When fabric binding is active, the active FBML is the list of fabric members with which the product is allowed to communicate. If fabric binding is disabled, this list is empty.
- **Pending FBML:** A list used to configure an FBML before it is made active on the product. Changes to the pending FBML are not implemented in the fabric until they are saved and activated using the `config.security.fabricBinding.activatePending` command as documented on page 2-53.

The following terms apply to the switches and directors that are part of the FBMLs:

- **Local:** The switch or director product that you are configuring. This is a required FBML member.
- **Attached:** A switch or director that is currently in a fabric with the local product. Any switch and director that is attached is a required FBML member.
- **Unattached:** A switch or director that is not currently in a fabric with the local product. These switches and directors are unattached if they have been added manually to the pending FBML, or if they segmented from the local fabric.

Enable/Disable and Online State Functions

In order for Fabric Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features when the director or switch is offline or online. Be aware of the following:

- Because switches are bound to a fabric by World Wide Name (WWN) and domain ID, the Insistent Domain ID option in the *Configure Switch Parameters* dialog box is automatically enabled if Fabric Binding is enabled. You cannot disable Insistent Domain ID while Fabric Binding is active and the switch is online.
- If Fabric Binding is enabled and the switch is online, you cannot disable Insistent Domain ID.
- If Fabric Binding is enabled and the director is offline, you can disable Insistent Domain ID, but this will disable Fabric Binding.
- You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding.

NOTE: Fabric Binding can be disabled when the switch is offline.

config.security.fabricBinding.activatePending

Syntax activatePending

Purpose This command activates the fabric binding configuration contained in the pending work area to the fabric. The Pending FBML becomes the Active FBML, and fabric binding is made functional.

NOTE: This command takes effect immediately. The CLI verifies the list before activating it to the fabric.

Parameters This command has no parameters.

Command Example **Root>** config security fabricBinding activatePending

config.security.fabricbinding.addAttachedMembers

Syntax addAttachedMembers

Purpose This command adds all the current members of the fabric to the Pending FBML. If a fabric member's domain ID or WWN already exists in the list, it is not added.

Parameters This command has no parameters.

Command Example **Root>** config security fabricbinding addAttachedMembers

config.security.fabricBinding.addMember

Syntax `addMember wwn domainId`

Purpose This command adds a new member to the Pending FBML in the fabric binding work area. The number of entries is limited to the maximum available domain IDs for the fabric, which is 239.

NOTE: Changes from this command are not activated to the fabric until the `activatePending` command is issued.

Parameters This command has two parameters:

<code>wwn</code>	Specifies the world wide name (WWN) of the member to be added to the Pending FBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).
<code>domainId</code>	The domain ID of the member to be added to the Pending FBML. Valid domain IDs range from 1 to 239.

Command Example **Root>** `config security fabricBinding addMember
AA:99:23:23:08:14:88:C1 2`

config.security.fabricBinding.clearMemList

Syntax `clearMemList`

Purpose This command clears the Pending FBML in the working area. Members that are attached remain in the list, because the Pending FBML must contain all attached members to become active.

NOTE: This information is not saved to the fabric until the `activatePending` command is issued. When the list is cleared, the CLI automatically adds the managed switch to the Pending FBML.

Parameters This command has no parameters.

Command Example **Root>** `config security fabricBinding clearMemList`

config.security.fabricbinding.deactivateFabBind

Syntax deactivateFabBind

Purpose This command deactivates the active FBML on the fabric. The Active FBML is erased when this command is executed.

NOTE: This command takes effect immediately in the fabric.

Parameters This command has no parameters.

Command Example **Root>** config security fabricbinding deactivateFabBind

config.security.fabricBinding.deleteMember

Syntax deleteMember wwn domainId

Purpose This command removes a member from the Pending FBML in the fabric binding work area. The local member and attached members cannot be deleted from the list.

NOTE: Changes are not activated to the fabric until the activatePending command is issued.

Parameters This command has two parameters:

wwn Specifies the WWN of the member to be removed from the Pending FBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).

domainId The domain ID of the member to be removed from the Pending FBML. Valid domain IDs range from 1 to 239.

Command Examples **Root>** config security fabricBinding deleteMember
AA:99:23:23:08:14:88:C1
Root> config security fabricBinding deleteMember 2

config.security.fabricBinding.replacePending

Syntax `replacePending`

Purpose This command replaces the Pending FBML with the fabric binding configuration that is currently loaded on the fabric.

Parameters This command has no parameters.

Command Example **Root>** `config security fabricBinding replacePending`

config.security.fabricBinding.showActive

Syntax `showActive`

Purpose This command displays the fabric binding configuration (active FBML) saved on the fabric. It performs the same function as [show.security.fabricBinding](#) on page 2-180.

Parameters This command has no parameters.

Output This command displays the following fabric binding configuration data:

Domain ID	The domain ID of the FBML member. Valid domain ID's range from 1 to 239.
WWN	The world wide name (WWN) of the FBML member in colon-delimited hexadecimal notation.
Attachment Status	Indicates whether the FBML member is Local, Attached, or Unattached. For more information, see Fabric Binding Membership Terminology on page 2-51.

Output Example The output from the `config.security.fabricBinding.showActive` command displays as follows.

```
Domain 1  (20:30:40:50:60:70:8F:1A)  (Local)
Domain 3  (00:11:22:33:44:55:66:77)  (Unattached)
Domain 2  (88:99:AA:BB:CC:DD:EE:FF)  (Attached)
Domain 14 (11:55:35:45:24:78:98:FA)  (Attached)
```

config.security.fabricBinding.showPending

Syntax `showPending`

Purpose This command displays the pending FBML, which may not reflect what is active on the fabric.

Parameters This command has no parameters.

Output The fabric binding configuration data is displayed as a table that includes the following properties of the Pending FBML.

Domain ID	The domain ID of the FBML member. Valid domain ID's range from 1 to 239.
WWN	The world wide name (WWN) of the FBML member in colon-delimited hexadecimal notation.
Attachment Status	Indicates whether the FBML member is Local, Attached, or Unattached. For more information, see Fabric Binding Membership Terminology on page 2-51.

Output Example The output from the config.security.fabricBinding.showPending command displays as follows.

```
Domain 1  (20:30:40:50:60:70:8F:1A)  (Local)
Domain 3  (00:11:22:33:44:55:66:77)  (Unattached)
Domain 2  (88:99:AA:BB:CC:DD:EE:FF)  (Attached)
Domain 14 (11:55:35:45:24:78:98:FA)  (Attached)
```

config.security.portBinding

The Port Binding CLI commands enable you to “bind” a specific switch or director port to the WWN of an attached node, switch, or director for exclusive communication.

config.security.portBinding.bound

Syntax `bound portNumber portBindingState`

Purpose This command sets the port binding state for a given port.

Parameters This command has two parameters.

portNumber	Specifies the port number for which the port binding state is being set. Valid port number values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portBindingState	Specifies the port binding state as active or inactive. Valid values are <i>true</i> and <i>false</i> . <i>true</i> sets the port binding to active. The specified port is bound to the WWN configured with the config.security.portBinding.wwn command. If no WWN has been configured, no devices can log in to that port. <i>false</i> sets the port binding to inactive. Any device is free to connect to the specified port in this state, regardless of the WWN setting. Boolean 1 and 0 may be substituted as values.

Command Examples **Root>** config security portBinding bound 4 true

Root> config security portBinding bound 4 1

config.security.portBinding.show

Syntax show portNumber

Purpose This command shows port binding configuration for a single port.

Parameters	This command has one parameter.	
	portNumber	Specifies the port number for which the port binding configuration will be shown. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command Example **Root>** config security portBinding show 4

Output The port binding configuration data is displayed as a table that includes the following properties.

Port Number	The port number.
WWN Binding	The state of port binding for the specified port, either active or inactive.
Bound WWN	The WWN of the device that is bound to the specified port. If this field is blank, no device has been bound to the specified port.

Output Example The output from the config.security.portBinding.show command displays as follows.

```
Port Number:      4
WWN Binding:      Active
Bound WWN:        AA:99:23:23:08:14:88:C1
```

config.security.portBinding.wwn

Syntax wwn portNumber boundWwn

Purpose This command configures the single device WWN to which a port is bound.

Parameters

This command has two parameters.

portNumber	<p>Specified the port number for which the bound WWN is being set. Valid port number values are:</p> <ul style="list-style-type: none"> 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
boundWwn	<p>Specifies the WWN of the device that is being bound to the specified port. The value must be entered in colon-delimited hexadecimal notation (for example, 11:22:33:44:55:66:AA:BB). If the boundWwn is configured and the portBindState is:</p> <ul style="list-style-type: none"> Active—only the device described by boundWwn is able to connect to the specified port. Inactive—the WWN is retained, but any device can connect to the specified port. <p>Instead of the WWN, either of two values can be entered in this parameter:</p> <ul style="list-style-type: none"> <i>attached</i> automatically configures the currently attached device WWN as the bound WWN. <i>remove</i> changes the WWN to the default value, 00:00:00:00:00:00:00:00. Even though this removes the WWN-port association, if the portBindingState value set with the config.security.portBinding.bound command is still <i>true</i> (the port binding is active), other devices are prevented from logging in to this port. To allow other devices to log in to this port, use the config.security.portBinding.bound command to set the portBindingState parameter to false.

Command Examples

```
Root> config security portBinding wwn 4
AA:99:23:23:08:14:88:C1
```

```
Root> config security portBinding wwn 4 attached
```

```
Root> config security portBinding wwn 4 remove
```

config.security.ssh.resetKeys

Syntax resetKeys

Purpose This command resets the SSH (secure shell) encryption keys to their factory default (unconfigured). The next time a client connects using SSH the server will generate new keys.

Parameters This command has no parameters

Command Example

```
Root> config security ssh resetKeys
```

config.security.ssh.setState

Syntax setState sshEnableState

Purpose This command sets the enabled state for the SSH interface. In order for an SSH client connection to be accepted, the state must be set to *enable*; otherwise, only Telnet can be accepted. Either SSH can be enabled, or Telnet can be enabled, but not both at the same time.

Parameters This command has one parameter:

sshEnableState This parameter can be set to *enable* or *disable*. Boolean 1 and 0 values may also be substituted.

Command Example

```
Root> config security ssh setState enable
```

config.security.ssh.show

Syntax show

Purpose This command displays SSH state.

Parameters This command has no parameters.

Command Example `config security ssh show`

Output The output of the `config.security.ssh.show` command displays the following data:

SSH	Indicates if the SSH interface to CLI is enabled or disabled.
Telnet	Indicates if the Telnet interface to CLI is enabled or disabled.

Output Example

SSH:	enabled
Telnet:	disabled

config.security.switchAcl

The access control list (ACL) feature allows a user with appropriate rights to configure a set of IP addresses that are allowed to make an IP management connection to the product.

config.security.switchAcl.addRange

Syntax `addRange startIPAddress endIPAddress`

Purpose This command adds a new range of IP addresses to the access control list.

Parameters This command has the following parameters:

startIPAddress	The starting IP Address of the desired range. The address must be entered in dotted decimal form (such as, 10.0.0.0).
endIPAddress	The ending IP Address of the desired range. The address must be entered in dotted decimal form (such as, 10.0.0.0).

The maximum number of entries in this command is 32.

NOTE: The starting IP address must be lesser than the ending IP address.

Command Example

```
Root> config security switchAcl addRange 10.0.0.0
10.0.0.2
```

config.security.switchAcl.deleteRange

Syntax `deleteRange startIPAddress endIPAddress`

Purpose This command deletes a range of IP addresses from the access control list. This range must exactly match one of the existing ranges in the access control list.

Parameters This command has the following parameters:

startIPAddress	The starting IP Address of the range to be deleted. The address must be entered in dotted decimal form (such as, 10.0.0.0). <i>clear</i> - Using the optional 'clear' parameter by itself will remove all of the entries from the access control list.
endIPAddress	The ending IP Address of the range to be deleted. The address must be entered in dotted decimal form (such as, 10.0.0.0).

Command Example

```
Root> config security switchAcl deleteRange 10.0.0.0
10.0.0.2
```

config.security.switchAcl.setState

Syntax `setState aclEnabledState`

Purpose This command sets the enabled state of the access control list. In order for the access control list to be enforced, the state must be set to *enable*.

Parameters This command has one parameter:

aclEnabledState	This parameter can be set to <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
-----------------	--

Command Example **Root>** config security switchAcl setState 1

config.security.switchAcl.show

Syntax show

Purpose This command displays the contents of the access control list.

Parameters This command has no parameters.

Command Example **Root>** config security switchACL show

Output This command displays the following access control list information:

Starting IP Address	The starting IP Address of the range in the access control list.
Ending IP Address	The ending IP Address of the range in the access control list.

Output Example The output from the config.security.switchAcl.show command displays as follows.

ACL State: Disabled

Starting IP Address	Ending IP Address
-----	-----
110.80.1.1	110.80.255.255
110.81.1.10	110.81.1.255
200.11.15.1	200.11.255.128

config.security.switchBinding

Switch Binding CLI commands allow you to enable the product to communicate only with nodes, switches, and directors that are listed on the Switch Binding Membership List (SBML). Switch Binding restricts connections to only the devices listed on the SBML and allows no other devices to communicate with the switch. When an unauthorized WWN attempts to log in, it is denied a connection and an event is posted to the Event Log. This provides security in environments that include a large number of nodes, switches, and directors by ensuring that only the specified set of WWNs are able to attach to the managed product.

You can use the Switch Binding commands to enable Switch Binding and to create and change the SBML. Switch Binding is available only if the SANtegrity Binding feature is installed.

Enable, Disable and Online State Functions

For Switch Binding to function, specific operating parameters and optional features must be enabled. Also, there are specific requirements for disabling these parameters and features:

- Switch Binding can be enabled or disabled whether the product is offline or online.
- Enabling Enterprise Fabric Mode automatically enables Switch Binding.
- You cannot disable Switch Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is online, you cannot disable Switch Binding.
- If Enterprise Fabric Mode is enabled and the director or switch is offline you can disable Switch Binding, but this also disables Enterprise Fabric Mode.
- WWNs can be added to the SBML without regard to whether Switch Binding is enabled or disabled.

config.security.switchBinding.addMember

Syntax `addMember wwn`

Purpose This command adds a new member to the SBML. A maximum number of 256 members may be added to the SBML.

Parameters This command has one parameter:

<code>wwn</code>	Specifies the switch or N_Port device WWN of the member to be added to the SBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).
------------------	---

Command Example

```
Root> config security switchBinding addMember
AA:99:23:23:08:14:88:C1
```

config.security.switchBinding.deleteMember

Syntax	deleteMember wwn	
Purpose	This command removes a member from the SBML. The user cannot remove any member currently logged into the switch.	
Parameters	This command has one parameter:	
	wwn	Specifies the switch or N_Port device WWN of the member to be removed from the SBML. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00). The user may also enter <i>all</i> for this argument to clear the SBML completely. Note that the user cannot clear a WWN that is currently logged into the switch.

Command Example

```
Root> config security switchBinding deleteMember  
AA:99:23:23:08:14:88:C1
```

config.security.switchBinding.setState

Syntax	setState switchBindingState
Purpose	This command sets the switch binding state on the switch.

Parameters This command has one parameter:

switchBindingState Sets the switch binding state for the switch. Valid values are:

- disable* - Disable switch binding. Devices (servers, storage, and other switches) are allowed to connect to the switch without restrictions.
- eRestrict* - Enable switch binding and restrict E_Port connections. E_Ports are prevented from forming ISL connections unless explicitly identified in the SBML. F_Port connections are allowed without restriction.
- fRestrict* - Enable switch binding and restrict F_Port connections. Server and (or) storage devices are prevented from forming F_Port connections with the switch unless explicitly identified in the SBML. E_Ports are allowed to form ISL connections without restriction.
- allRestrict* - Enable switch binding and restrict E_Port and F_Port connections. Both E_Ports and F_Ports prohibit connections with all devices unless explicitly identified in the SBML.

Command Example **Root>** config security switchBinding setState allRestrict

config.security.switchBinding.show

Syntax show

Purpose This command displays the switch binding configuration.

Parameters This command has no parameters.

Output This command displays the following switch binding configuration data:

switchBindingState	The state of switch binding, which can have the following values: Disabled, Enabled and Restricting F_Ports, Enabled and Restricting E_Ports, or Enabled and Restricting All Ports.
Switch Binding Membership List	The WWNs of members of the SBML saved on the switch.

Output Example The output from the config.security.switchBinding.show command displays as follows.

```
Switch Binding State:   Enabled and Restricting E Ports
00:11:22:33:44:55:66:77
88:99:AA:BB:CC:DD:EE:FF
11:55:35:45:24:78:98:FA
```

config.snmp.addCommunity

Syntax addCommunity commIndex commName writeAuthorization
trapRecipient udpPortNum

Purpose This command adds an SNMP community to the SNMP configuration.

Parameters This command has five parameters. Up to six community names and trap recipients may be defined.

commIndex	Specifies the community to be created or edited. Valid values are integers in the range 1–6.
commName	Specifies the community name of the community specified by commIndex. The community name must not exceed 32 characters in length. Valid characters include all those in the ISO Latin-1 character set. Duplicate community names are allowed, but the corresponding writeAuthorization values must match.
writeAuthorization	Specifies the write authorization state of the community. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.
trapRecipient	Specifies the trap recipient. Values must be 4 bytes in dotted-decimal format.
udpPortNum	Specifies the user datagram protocol (UDP) port number to which the director sends traps for each recipient. The value can be a decimal number or <i>default</i> . The default value is 162. Valid values include all legal UDP port numbers.

Command Example **Root>** config snmp addCommunity 1 CommunityName1 enabled
123.123.123.123 162

config.snmp.authTraps

Syntax authTraps enabledState

Purpose This command enables or disables the authentication traps to be sent to SNMP management stations when unauthorized stations try to access SNMP information from the director or switch.

Parameters	This command has one parameter.	
	enabledState	Specifies whether the authentication traps are enabled. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.

Command Examples

```
Root> config snmp authTraps enable
Root> config snmp authTraps 1
```

config.snmp.deleteCommunity

Syntax	deleteCommunity commIndex	
Purpose	This command entirely deletes a community from the SNMP.	
Parameters	This command has one parameter.	
	commIndex	Specifies the community to be deleted. Valid values are integers in the range 1–6. This value was set in the commIndex parameter of the config.snmp.addCommunity command. Valid values are integers in the range 1–6.

Command Example

```
Root> config snmp deleteCommunity 5
```

config.snmp.setFaMibVersion

Syntax	setFaMibVersion versionNumber	
Purpose	This command sets the version of the Fibre Alliance MIB with which the SNMP agent interacts. The version number can be set to 3.0 or 3.1.	
Parameters	This command has one parameter.	
	versionNumber	Sets the version of the Fibre Alliance MIB version number. Accepted values for this command are 3.0 or 3.1.

Command Example

```
Root> config snmp setFaMibVersion 3.1
```

config.snmp.setState

Syntax `setState enabledState`

Purpose This command enables or disables the SNMP agent. When disabled, the SNMP agent does not respond to any requests or send any traps.

Parameters This command has one parameter.

<code>enabledState</code>	Sets the state of the SNMP agent. This parameter can be set to <i>enable</i> or <i>disable</i> . Boolean 1 and 0 values may also be substituted.
---------------------------	--

Command Example

Root> `config snmp setState 1`

config.snmp.show

Syntax `show`

Purpose This command shows the switch SNMP configuration.

Parameters This command has no parameters.

Command Example

Root> `config snmp show`

Output The switch configuration data is displayed as a table that includes the following properties.

SNMP Agent State	The state of the SNMP agent. If it is disabled, the SNMP state does not respond to any requests and does not produce any traps.
------------------	---

FA MIB Version Number	Version of the MIB that the SNMP agent is configured to use.
-----------------------	--

Authentication Traps	The state of the authentication traps (for example, enabled) that are sent to SNMP management stations when unauthorized stations attempt to access SNMP information from the switch.
----------------------	---

Index	The community index number.
-------	-----------------------------

Community Name	The name of the community.
WriteAuth	The write authorization state.
Trap Recipient	The address of the trap recipient shown in 4-byte dotted-decimal format.
UDP Port	The user datagram protocol (UDP) port number to which the director will send traps for each recipient.

Output Example The output from the `config.snmp.show` command displays as follows.

```
SNMP Agent State:      Enabled
FA MIB Version Number: 3.0
Authentication Traps:  Enabled
Index  Community Name      WriteAuth  Trap Recipient  UDP Port
-----
1      CommunityName1      Enabled    123.123.123.123  162
2      CommunityName2      Enabled    10.25.25.10     144
3      CommunityName3      Disabled   132.44.85.224   162
4      public              Enabled    132.44.85.224   162
5
6
```

config.switch

All commands under this branch operate on a particular switch attribute. Switch attributes are those attributes that are specific to the Fibre Channel switch nature of the product.

Some of the `config.switch` commands require that the switch be set offline. (Use the `maint.system.setOnlineState` to set the switch offline.) If these commands are entered while the switch is online, an error message results.

config.switch.domainRSCN

Syntax `domainRSCN domainRSCNState`

Purpose This command sets the domain RSCN state for the switch. The switch can be either offline or online when this command is executed. When this parameter is enabled, domain register for state change notifications (domain RSCNs) are sent between end devices in a

fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port.

Parameters This command has one parameter.

domainRSCNState Specifies whether the domain RSCN state is enabled. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command Example **Root>** config switch domainRSCN 1

config.switch.edTOV

Syntax edTOV timeoutValue

Purpose This command sets the E_D_TOV for the switch.

NOTE: The switch must be set offline before this command is entered.

Special care should be used when scripting this command due to its relationship with R_A_TOV.

Parameters This command has one parameter.

timeoutValue Specifies the new E_D_TOV value. The units for this value are tenths of a second. This parameter must be an integer in the range 2–600 (0.2 second to 60 seconds), and it must be smaller than the R_A_TOV.

Command Example **Root>** config switch edTOV 4

config.switch.insistDomainId

Syntax insistDomainId insistentDomainIdState

Purpose This command sets the insistent domain ID state for the switch.

Parameters This command has one parameter.

insistentDomainIdState Specifies whether the insistent domain ID state is enabled. Valid values are *enable* and *disable*. Boolean 1 and 0 may be substituted as values.

Command Example **Root>** config switch insistDomainId 1

NOTE: The Insistent Domain ID must be enabled, if the Enterprise Fabric Mode (an optional SANtegrity feature) or Preferred Path is enabled.

config.switch.interopMode

Syntax interopMode interopMode

Purpose This command sets the interoperability mode for the switch. The switch must be offline to complete this command.

NOTE: The switch must be set offline before this command is entered.

Parameters This command has one parameter.

interopMode Specifies the interoperability mode. Valid values are *mcdata* and *open*:
mcdata — McDATA Fabric 1.0. Select this mode if the fabric contains only McDATA switches and directors that are also operating in McDATA Fabric 1.0 mode.
open — Open Fabric 1.0. Select this mode if the fabric contains McDATA switches and directors and other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.

Command Example **Root>** config switch interopMode open

config.switch.ltdFabRSCN

Syntax ltdFabRSCN ltdFabRSCNState

Purpose This command sets the status of limited fabric RSCNs. When enabled, fabric register for state change notifications (RSCNs) are suppressed during an IPL.

Parameters This command has one parameter.

<code>ltdFabRSCNState</code>	Specifies whether the limited fabric RSCN state is enabled. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.
------------------------------	---

Command Example `Root> config switch ltdFabRSCN 1`

config.switch.prefDomainId

Syntax `prefDomainId domainId`

Purpose This command sets the preferred domain ID for the switch. The switch must be offline to complete this command.

NOTE: The switch must be set offline before this command is entered.

Parameters This command has one parameter.

<code>domainId</code>	Specifies the new preferred domain ID value. This parameter must be an integer in the range 1–31.
-----------------------	---

Command Example `Root> config switch prefDomainId 1`

config.switch.priority

Syntax `priority Priority`

Purpose This command sets the switch priority.

NOTE: The switch must be set offline before this command is entered.

Parameters

This command has one parameter.

Priority

Specifies the switch priority. Valid values are: *principal*, *default*, or *neverprincipal*.

principal — sets the numerical switch priority to 1. The switch with a priority of 1 becomes the principal switch; however, if two or more switches have a priority of 1, the switch with the lowest WWN becomes the principal switch.

default — sets the numerical switch priority to 254. If no switch is set to principal, the switch with a priority 254 becomes the principal switch; however, if two or more switches have a priority of 254, the switch with the lowest WWN becomes the principal switch.

neverprincipal — sets the numerical switch priority to 255. This switch is not able to become the principal switch.

At least one switch in a multiswitch fabric must have a switch priority value of *principal* or *default*.

The number codes 2–253 are not now in use.

Command Example

```
Root> config switch priority principal
```

config.switch.raTOV**Syntax**

```
raTOV timeoutValue
```

Purpose

This command sets the R_A_TOV for the switch.

NOTE: The switch must be set offline before this command is entered.

Special care should be used when scripting this command due to its relationship with E_D_TOV.

Parameters This command has one parameter.

timeoutValue	Specifies the new R_A_TOV value. The units for this value are tenths of a second. This parameter must be an integer in the range 10–1200 (1 second to 120 seconds), and it must be larger than the E_D_TOV.
--------------	---

Command Example `Root> config switch raTOV 20`

config.switch.rerouteDelay

Syntax `rerouteDelay rerouteDelayState`

Purpose This command enables or disables rerouting delay for the switch.

NOTE: The switch can be either offline or online when this command is executed.

This command is only applicable if the configured switch is in a multiswitch fabric. Enabling the rerouting delay ensures that frames are delivered in order through the fabric to their destination.

If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order because frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

If rerouting delay is enabled, traffic ceases in the fabric for the time specified in the config.switch.edTOV command. This delay allows frames sent on the old path to exit to their destination before new frames begin traversing the new path. Note that during this delay period, frames addressed to the destinations that are being rerouted are discarded if they are Class 3 frames and rejected if they are Class 2 or Class F frames.

Parameter	This command has one parameter.	
	rerouteDelayState	Specifies whether rerouting delay is enabled. Valid values are <i>true</i> and <i>false</i> . Boolean 1 and 0 may be substituted as values.

Command Examples

```
Root> config switch rerouteDelay true
Root> config switch rerouteDelay 1
```

config.switch.speed

Syntax speed switchSpeed

Purpose This command sets the speed for the switch.

NOTE: This command is only applicable for the Intrepid 6064.

NOTE: The switch must be set offline before this command is entered.

A switch can be configured to operate at 1 Gbps or 2 Gbps.

If the switch has FPM cards, configuring the switch speed to 2 Gbps makes all the ports on the FPM cards inactive, and their operational state will be set to inactive. FPM ports do not support 2 Gbps and, therefore, will remain inactive after the switch is returned to the online state.

Parameters	This command has one required parameter.	
	switchSpeed	Specifies the speed of the switch. Valid values are 1 G/sec or 2 G/sec.

Command Examples

```
Root> config switch speed 2g
```

config.switch.show

Syntax show

Purpose This command shows the switch configuration.

NOTE: The switch can be either offline or online when this command is executed.

Parameters This command has no parameters.

Command Example **Root>** config switch show

Output The switch configuration data is displayed as a table that includes the following properties.

BB Credit	The maximum number of outstanding frames that can be transmitted without causing a buffer overrun condition at the receiver. (This is not valid for the Sphereon 4300 and Sphereon 4500 switches.)
R_A_TOV	Resource Allocation Time Out Value. This value is set in tenths of a second.
E_D_TOV	Error Detect Time Out Value. This value is set in tenths of a second.
Preferred Domain Id	The preferred domain ID of the switch.
Switch Priority	The switch priority. Values are Principal, Default, or Never Principal.
Speed	The switch speed. (This is not valid for the Sphereon 4300 and Sphereon 4500 switches.)
Rerouting Delay	The rerouting delay that ensures that frames are delivered in order through the fabric to their destination. Values are Enabled or Disabled.
Interop Mode	Interoperability mode for the switch.
Insistent Domain Id	When enabled, ensures that the embedded firmware cannot change a switch's preferred domain ID.
Domain RSCN	When enabled, allows domain RSCNs to be sent to registered members of the fabric.

Zoning RSCN	When enabled, allows zoning RSCNs to be sent to registered members of the fabric.
Limited Fabric RSCN	When enabled, fabric RSCNs are suppressed after an IPL.
Zone Flex Pars	When set to fabric, RSCNs will only be sent to affected fabric members when zoning information changes. When set to none, filtering of RSCNs will not take place, and RSCNs will be sent to all zoneset members when zoning information changes.

Output Example The output from the config.switch.show command displays as follows.

```
BB Credit:                2
R_A_TOV:                  20
E_D_TOV:                   4
Preferred Domain Id: 1
Switch Priority:           Principal
Speed:                     2 Gb/sec
Rerouting Delay:          Enabled
Interop Mode:              Open Fabric 1.0
Insistent Domain Id: Disabled
Domain RSCN:               Enabled
Zoning RSCN:               Disabled
Limited Fabric RSCN: Disabled
Zone FlexPars:             Fabric
```

config.switch.zoneFlexPars

Syntax zoneFlexPars zoneFlexParstate

Purpose This command configures the state of Zone Flex Pars.

Parameters	This command has one parameter:
zoneFlexParsState	This parameter can be set to fabric and none. When set to fabric, RSCNs will only be sent to affected fabric members when zoning information changes. When set to none, filtering of RSCNs will not take place, and RSCNs will be sent to all zoneset members when zoning information changes

Command Example **Root>** config switch zoneFlexPars fabric

config.switch.zoningRSCN

Syntax	zoningRSCN zoningRSCNState
Purpose	This command sets the zoning RSCN state for the switch. When enabled, this parameter allows zoning register for state change notifications (RSCNs) to be sent to registered members of the fabric. Zoning RSCNs are sent to ports on the switch following any change to the fabric's active zone set. The switch can be either offline or online when this command is executed.
Parameters	This command has one parameter.
zoningRSCNState	Specifies whether the zoning RSCN state is enabled. Valid values are <i>enable</i> , <i>disable</i> , <i>true</i> , and <i>false</i> . Boolean 1 and 0 may be substituted as values.

Command Example **Root>** config switch zoningRSCN 1

config.system.contact

Syntax	contact systemContact
Purpose	This command sets the system contact attribute.

Parameters This command has one parameter.

systemContact	Specifies the new system contact string for the director or switch. The contact can contain 0–255 characters.
---------------	---

Command Example **Root>** config system contact Joe

config.system.date

Syntax date systemDate systemTime

Purpose This command sets the system date and time.

Parameters This command has two required parameters.

systemDate	Specifies the new system date. The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. Valid date values include: mm: 1–12 dd: 1–31 yyyy: >1980
systemTime	Specifies the new system time. The format of the time parameter must be hh:mm:ss. Valid time values include: hh: 0–23 mm: 0–59 ss: 0–59

Command Examples **Root>** config system date 04:16:2001 10:34:01

Root> config system date 10/09/2001 14:07:55

config.system.description

Syntax description systemDescription

Purpose This command sets the system description string.

Parameters This command has one parameter.

systemDescription Specifies the new system description string for the director or switch. The name can contain 0–255 characters.

Command Example **Root>** config system description McDATA Intrepid 6064
Fibre Channel Director

config.system.location

Syntax location systemLocation

Purpose This command sets the system location attribute.

Parameters This command has one parameter.

systemLocation Specifies the new system location for the director or switch. The location can contain 0–255 characters.

Command Example **Root>** config system location Everywhere

config.system.name

Syntax name systemName

Purpose This command sets the system name attribute.

Parameters This command has one required parameter.

systemName Specifies the new system name for the director or switch. The name can contain 0–24 characters.

Command Example **Root>** config system name Joe's Switch

config.system.show

Syntax show

Purpose This command shows the system configuration.

Parameters This command has no parameters.

Command Example **Root>** config system show

Output The system configuration is displayed as a table that includes the following properties.

Name	The system name.
Description	The system description.
Contact	The system contact.
Location	The system location.
Date/Time	The system date and time.

Output Examples The output from the config.system.show command displays as follows.

```

Name:          Joe's Switch
Description:    McDATA Intrepid 6064 Fibre Channel Director
Contact:        Joe
Location:       Everywhere
Date/Time:      04/16/2001  10:34:01

```

config.zoning

Note that the config.zoning commands function in a different way from most CLI commands, which are single action commands that take effect immediately. A zoning configuration is typically too complicated to be described by a single command, so the first zoning command entered invokes a work-area editor. The commands take effect on a temporary copy of a zone set in the work area until the temporary copy in the work area is activated to the fabric--or is discarded.

Because not all the verification of the zone set can occur on the temporary copy in the work area, it is possible, however unlikely, that the copy of the zone set encounters no errors until the zone set is activated to the fabric.

NOTE: Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode. In this case, you must use node WWNs as zone members.

NOTE: A Sphereon 4300 Switch cannot participate in a fabric, unless the Fabric Capable feature is enabled. For more information, see the *McDATA Sphereon 4300 Switch Installation and Service Manual* (620-000171).

Table 2-1 shows the limits for configuring zoning in McDATA fabrics that are supported by switch and director firmware as of 11/14/03. Although EFCM 8.0 or EFCM 8.0b may allow you to configure greater values in the Zoning Library, values in this table have been tested and are supported. For the latest limits, refer to the *Supported Fabrics Configuration Document* located on www.mcdata.com in the Resource Library or contact your customer support representative.

Table 2-1 Supported Zoning Configurations

Product	Intrepid 6064 Intrepid 6140	Sphereon 4500	Sphereon 3x32 Sphereon 3x16	ED-5000
Number of End Ports	1024	1024	1024	1024
Unique Zone Members	1024	1024	1024	1024
Members per Zone	1024	1024	1024	1024
Zones	1024	1024	1024	512

config.zoning.activateZoneSet

Syntax activateZoneSet

Purpose This command activates the zone set contained in the work area to the fabric and takes effect immediately.

NOTE: This command takes effect immediately in the fabric.

Parameters This command has no parameters.

Command Example **Root>** config zoning activateZoneSet

NOTE: If the interoperability mode for the switch or director is set to Open Fabric 1.0 mode when the zone is activated, any zone members specified by port number are ignored.

config.zoning.addPortMem

Syntax addPortMem "zoneName" domainId portNumber

Purpose This command adds the domain ID and port number of a zone member to the specified zone in the work area.

NOTE: Port numbers cannot be used for zone members if the interoperability mode for the switch or director is set to Open Fabric 1.0 mode.

NOTE: A product can have at most 1024 zone members in its zones.

NOTE: The ED-5000 supports a maximum of 512 zones.

Parameters This command has the following parameters.

zoneName	Specifies the name of the zone.
domainId	Specifies the domain ID of the member to be added to the zone. Valid values are in the range 1–31.
portNumber	Specifies the port number of the member to be added to the zone. Valid port number values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command Example **Root>** config zoning addPortMem TheUltimateZone 10 6

config.zoning.addWwnMem

Syntax `addWwnMem zoneName wwn`

Purpose This command adds a WWN zone member to the specified zone in the work area.

NOTE: A product can have at most 1024 zone members in its zones.

NOTE: The ED-5000 supports a maximum of 512 zones.

Parameters This command has two parameters.

zoneName Specifies the name of the zone.

wwn The WWN of the member to be added to the zone. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).

Command Example **Root>** `config zoning addWwnMem TheUltimateZone
10:00:00:00:C9:22:9B:64`

config.zoning.addZone

Syntax `addZone zoneName`

Purpose This command adds a new (empty) zone to the zone set in the work area.

NOTE: Changes are not activated on the switch until the `config.zoning.activateZoneSet` command is issued.

NOTE: A zone set can have a maximum of 1024 zones.

NOTE: A Switch or Director can have a maximum of 1024 zone members in all of its zones, except for the ED-5000, which allows a maximum of 512 zones.

Parameters This command has one parameter.

zoneName	Specifies the name of the new zone. The zoneName must contain 1–64 characters. Valid characters are: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789\$-^_ Spaces are not permitted, and the first character must be alphabetical.
----------	--

Command Example `Root> config zoning addZone TheUltimateZone`

config.zoning.clearZone

Syntax `clearZone zoneName`

Purpose This command clears all zone members for the specified zone in the work area. This command does not change the zone name.

Parameters This command has one parameter.

zoneName	Specifies the name of the zone to be cleared.
----------	---

Command Example `Root> config zoning clearZone TheNotUltimateAtAllZone`

config.zoning.clearZoneSet

Syntax `clearZoneSet`

Purpose This command clears the zone set contained in the work area, removing all zones, and takes effect immediately. This command does not change the zone set name.

Parameters This command has no parameters.

Command Example `Root> config zoning clearZoneSet`

config.zoning.deactivateZoneSet

Syntax deactivateZoneSet

Purpose This command places all attached devices in the default zone and takes effect immediately for the entire fabric. This command clears both the active zone set and the working area. This command takes effect immediately in the fabric.

NOTE: The default zone must be activated independently of this command.

Parameters This command has no parameters.

Command Example **Root>** config zoning deactivateZoneSet

config.zoning.deletePortMem

Syntax deletePortMem zoneName domainId portNumber

Purpose This command deletes a domain ID and port number for a zone member in the specified zone in the work area.

Parameters This command has three parameters.

zoneName	Specifies the name of the zone that contains the member to be deleted.
domainId	Specifies the domain ID of the member that to be deleted from the zone. Valid domain IDs are in the range 1–31.
portNumber	Specifies the port number of the member to be deleted from the zone. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command Example **Root>** config zoning deletePortMem TheUltimateZone 10 5

config.zoning.deleteWwnMem

Syntax `deleteWwnMem zoneName wwn`

Purpose This command removes a WWN member from a zone that is in the work area.

Parameters This command has two parameters.

zoneName	Specifies the name of the zone that contains the member to be deleted.
wwn	Specifies the WWN of the member to be deleted from the zone. The value of the WWN must be in colon-delimited hexadecimal notation (for example, AA:00:AA:00:AA:00:AA:00).

Command Example **Root>** `config zoning deleteWwnMem TheNotSoUltimateZone 10:00:00:00:C9:22:9B:AB`

config.zoning.deleteZone

Syntax `deleteZone zoneName`

Purpose This command deletes a zone from the zone set in the work area.

NOTE: Changes are not activated on the switch until the `config.zoning.activeZoneSet` command is issued.

Parameters This command has one parameter.

zoneName	Specifies the name of the zone to be deleted.
----------	---

Command Example **Root>** `config zoning deleteZone TheLeastUltimateZone`

config.zoning.renameZone

Syntax `renameZone oldZoneName newZoneName`

Purpose This command renames a zone in the work area.

Parameters This command has two parameters.

oldZoneName	Specifies the current zone name of the zone to be renamed.
newZoneName	Specifies the new zone name. The newZoneName must contain 1–64 characters. Valid characters are: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789\$-^_ Spaces are not permitted, and the first character must be alphabetical.

Command Example **Root>** `config zoning renameZone TheOldUltimateZone
TheUltimateZone`

config.zoning.renameZoneSet

Syntax `renameZoneSet zoneSetName`

Purpose This command changes the name of the zone set in the work area.

NOTE: Changes are not activated on the switch until the `config.zoning.activateZoneSet` command is issued.

Parameters This command has one parameter.

zoneSetName	Specifies the new name for the zone set. The zoneSetName must contain 1–64 characters. Valid characters are: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789\$-^_ Spaces are not permitted, and the first character must be alphabetical.
-------------	--

Command Example **Root>** config zoning renameZoneSet TheUltimateZoneSet

config.zoning.replaceZoneSet

Syntax replaceZoneSet

Purpose This command replaces the work area with the active zone set that is currently loaded on the fabric.

Parameters This command has no parameters.

Command Example **Root>** config zoning replaceZoneSet

config.zoning.setDefZoneState

Syntax setDefZoneState defaultZoneState

Purpose This command enables or disables the default zone and takes effect immediately fabric wide.

NOTE: This command takes effect immediately in the fabric.

Parameters This command has one parameter.

defaultZoneState Specifies whether the default zone is enabled. Valid values are *true* and *false*. Boolean 1 and 0 may be substituted as values.

Command Examples **Root>** config zoning setDefZoneState false

Root> config zoning setDefZoneState 0

config.zoning.showActive

Syntax showActive

Purpose This command shows the zoning configuration saved on the fabric.

Parameters This command has no parameters.

Command Example **Root>** config zoning showActive

Output The zoning configuration data is displayed as a table that includes the following properties.

Active ZoneSet The enabled status, name, and member zones of the zone set.

Output Example The output from the `config.zoning.showActive` command displays as follows.

```
Active Zone Set
Default Zone Enabled:  False
ZoneSet:  TheUltimateZoneSet
  Zone:  TheUltimateZone
    ZoneMember: Domain 10, Port 6
    ZoneMember: Domain 15, Port 2
    ZoneMember: Domain 2, Port 63
    ZoneMember: 10:00:00:00:C9:22:9B:64
    ZoneMember: 10:00:00:00:C9:22:9B:BD
  Zone:  TheNotSoUltimateZone
    ZoneMember: 10:00:00:00:C9:22:9B:AB
    ZoneMember: 10:00:00:00:C9:22:9B:C6
    ZoneMember: 10:00:00:00:C9:22:9B:AB
  Zone:  TheNotUltimateAtAllZone
    ZoneMember: Domain 2, Port 63
```

config.zoning.showPending

Syntax `showPending`

Purpose This command shows the zoning configuration in the work area of the zone set that has not yet been activated.

Parameters This command has no parameters.

Command Example `Root> config zoning showPending`

Output The zoning configuration data is displayed as a table that includes the following properties.

Local ZoneSet The enabled status, name, and member zones of the zone set.

Output Example The output from the `config.zoning.showPending` command displays as follows.

```
Pending Zone Set
Default Zone Enabled: False
ZoneSet: TheNewUltimateZoneSet
  Zone: TheNewUltimateZone
    ZoneMember: Domain 10, Port 6
    ZoneMember: Domain 15, Port 2
  Zone: TheNewNotSoUltimateZone
    ZoneMember: 10:00:00:00:C9:22:9B:AB
    ZoneMember: 10:00:00:00:C9:22:9B:C6
    ZoneMember: 10:00:00:00:C9:22:9B:AB
  Zone: TheNewNotUltimateAtAllZone
    ZoneMember: Domain 2, Port 63
```

maint

The maint branch of the CLI command tree contains commands that relate to maintenance activities.

The commands in the maint branch can be used only by the administrator.

Note that the maint.system.resetConfig command resets all configuration data and non-volatile settings, including network information, to their default values (factory settings). Management access may be lost until the network information is restored.

maint.port.beacon

Syntax `beacon portNumber beaconState`

Purpose This command enables or disables port beaconing for a port.

Parameters This command has two required parameters.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
beaconState	Specifies whether beaconing is enabled. Valid values are <i>true</i> and <i>false</i> . Boolean 1 and 0 may be substituted as values.

Command Examples `Root> maint port beacon 4 false`

`Root> maint port beacon 4 0`

maint.port.reset

Syntax `reset portNumber`

Purpose This command resets a port.

This command resets an individual port without affecting any other ports. However, if a device is attached to the port and the device is online, the reset causes a link reset to occur. If the port is in a failed state (that is, after failing a loopback test), the reset restores the port to an operational state. The reset also clears all statistics counters and disables port beaconing for the specified port.

Parameters This command has one parameter.

portNumber	Specifies the port number to be reset. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
------------	---

Command Example **Root>** `maint port reset 4`

maint.system.beacon

Syntax `beacon beaconState`

Purpose This command enables or disables unit beaconing.

Parameters This command has one parameter.

beaconState	Specifies whether unit beaconing is enabled. Valid values are <i>true</i> and <i>false</i> . Boolean 1 and 0 may be substituted as values.
-------------	--

Command Examples **Root>** `maint system beacon false`

Root> `maint system beacon 0`

maint.system.clearSysError

Syntax `clearSysError`

Purpose This command clears the system error light.

Parameters This command has no parameters.

Command Example **Root>** `maint system clearSysError`

maint.system.ipl

Syntax `ipl`

Purpose This command IPLs the switch.

ATTENTION! Connection to the CLI is lost when this command runs.

Parameters This command has no parameters.

Command Example **Root>** `maint system ipl`

maint.system.resetConfig

Syntax `resetConfig`

Purpose This command resets all NV-RAM configuration parameters to their default values, including feature keys and IP addresses.

NOTE: This command IPLs the switch. Connection from the CLI to the switch is lost when this command runs.

ATTENTION! This command resets all configuration data and non-volatile settings, including network information, to their default values (factory settings). Management access may be lost until the network information is restored.

The default values are set in the firmware of the director or switch. For information about the default values, refer to the service manual for your director or switch.

Parameters This command has no parameters.

Command Example **Root>** maint system resetConfig

maint.system.setOnlineState

Syntax setOnlineState onlineState

Purpose This command sets the switch online or offline.

Parameters This command has one parameter.

onlineState	Specifies whether the switch is online. Valid values are <i>true</i> and <i>false</i> . Boolean 1 and 0 may be substituted as values.
-------------	---

Command Examples **Root>** maint system setOnlineState true

Root> maint system setOnlineState 1

perf

The perf branch of the CLI command tree contains commands that relate to performance services.

The commands in the perf branch can be used by either the administrator or the operator.

The counters in perf command output are 32-bit values that wrap at 4,294,967,296. To calculate the full value of a counter, multiply 4,294,967,296 by the value in the wrap field, and add the resulting product to the value in the count field. For example, if a TxFrames statistic has a count value of 1842953 and a wrap value of 12, the full value of the counter is:

$$(4,294,967,296 \times 12) + 1842953 = 51,541,450,505.$$

perf.class2

Syntax	class2 portNumber		
Purpose	This command displays port Class 2 counters for a single port.		
Parameters	<p>This command has one parameter.</p> <table><tr><td>portNumber</td><td>Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140</td></tr></table>	portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140		

Command Example **Root>** perf class2 2

Output	<p>The port Class 2 counter data is displayed as a table that includes the following statistics, along with a wrap count for each corresponding counter.</p> <table><tr><td>Port</td><td>The port number.</td></tr><tr><td>RxFrames</td><td>The number of Fibre Channel Class 2 frames that the port has received.</td></tr></table>	Port	The port number.	RxFrames	The number of Fibre Channel Class 2 frames that the port has received.
Port	The port number.				
RxFrames	The number of Fibre Channel Class 2 frames that the port has received.				

TxFrames	The number of Fibre Channel Class 2 frames that the port has transmitted.
RxWords	The number of Class 2 4-byte words within frames that the port has received.
TxWords	The number of Class 2 4-byte words within frames that the port has transmitted.
Busied Frms	The number of times that FBSY (Fabric Busy link response) was returned to this port as a result of a Class 2 frame that could not be delivered to the other end of the link. This occurs if either the fabric or the destination port is temporarily busy.
Rjct Frames	The number of times that FRJT (Frame Reject link response) was returned to this port as the result of a Class 2 frame that was rejected by the fabric.

Output Example The output from the perf.class2 command displays as follows.

```
Port 2
Statistic      Wrap      Count
-----
RxFrames       23        2953184
TxFrames       12        1842953
RxWords        65        2953184
TxWords        32        1842953
Busied Frms    0         2953184
Rjct Frames    0         1842953
```

perf.class3

Syntax class3 portNumber

Purpose This command displays port Class 3 counters for a single port.

Parameters This command has one parameter.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
------------	---

Command Example `Root> perf class3 2`

Output The port Class 3 counter data is displayed as a table that includes the following statistics, along with a wrap count for each corresponding counter.

Port	The port number.
RxFrames	The number of Fibre Channel Class 3 frames that the port has received.
TxFrames	The number of Fibre Channel Class 3 frames that the port has transmitted.
RxWords	The number of Class 3 4-byte words within frames that the port has received.
TxWords	The number of Class 3 4-byte words within frames that the port has transmitted.
Disc Frames	The number of Class 3 frames that have been discarded upon receipt by this port. There are no FBSYs (Fabric Busy link response) or FRJTs (Frame Reject link response) generated for Class 3 frames.

Output Example

The output from the perf.class3 command displays as follows.

Port 2 Statistic	Wrap	Count
-----	-----	-----
RxFrames	3	2953184
TxFrames	2	1842953
RxWords	65	2953184
TxWords	32	1842953
Disc Frames	26	2953184

perf.clearStats**Syntax**

`clearStats portNumber`

Purpose

This command resets all port statistics for an individual port or for all ports.

Parameters

This command has one parameter.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> for every port on the director or switch
------------	--

Command Example

Root> `perf clearStats 4`

Root> `perf clearStats all`

perf.errors**Syntax**

`errors portNumber`

Purpose

This command displays port error counters for a single port.

Parameters This command has one parameter.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
------------	---

Command Example `Root> perf errors 2`

Output The port error counter data is displayed as a table that includes the following statistics.

Port	The port number.
Prim Seq Err	The number of state machine protocol errors detected by the port hardware.
Disc Frms	The number of received frames discarded due to a frame size of less than size words or to frames dropped because the BB_Credit was zero. This number is counted during the first round of frame verification and applies to both Class 2 and Class 3 traffic.
Inv Tx Wrds	The number of 10-bit transmission words that the port is unable to map to 8-bit bytes because of disparity errors or misaligned K characters while in the OL2 or OL3 state.
CRC Errs	The number of frame CRC errors detected by the port.
Delim Errs	The number of invalid frame delimiters (SOF or EOF) received by the port.
Addr Id Errs	The number of frames received with unknown addressing.
FrmsTooShrt	The number of frames received that are too short.

Output Example

The output from the perf.errors command displays as follows.

```

Port 2
Statistic                Count
-----
Prim Seq Err             753452
Disc Frms                351269
Inv Tx Wrds              2953184
CRC Errs                 1842953
Delim Errs               2953184
Addr Id Errs             1842953
FrmsTooShrt              40059

```

perf.link**Syntax**

link portNumber

Purpose

This command displays port link counters for a single port.

Parameters

This command has one parameter.

portNumber	Specifies the port number. Valid values are:
	0–11 for the Sphereon 4300
	0–15 for the Sphereon 3016 and 3216
	0–23 for the Sphereon 4500
	0–31 for the Sphereon 3032 and 3232
	0–63 for the Intrepid 6064
	0–127 and 132–143 for the Intrepid 6140

Command Example

Root> perf link 2

Output

The port link counter data is displayed as a table that includes the following statistics.

Port	The port number.
OLS In	The number of offline sequences initiated by the attached N_Port.
OLS Out	The number of offline sequences initiated by this director or switch port.
Reset In	The number of link resets initiated by the attached N_Port.

Reset Out	The number of link resets initiated by this director or switch.
LIPS In	The number of Loop Initialization Primitives (LIPS) detected on this switch loop port.
LIPS Out	The number of LIPS generated on this switch loop port.
Link Flrs	The number of times the port has detected a link error resulting from an invalid link state transition or timeout.
Sync Losses	The number of times the port has detected a loss of synchronization timeout while not in an offline or LF2 state.
Sig Losses	The number of times the port has detected a loss of signal while not in an offline or LF2 state.
Time at 0 Tx Credit	The number of 100 millisecond intervals where the switch port has zero Tx BB credit.

Output Example The output from the perf.link command displays as follows.

```

Port 2
Statistic          Count
-----
OLS In             753452
OLS Out            351269
Reset In           2953184
Reset Out           1842953
Link Flrs           2953184
Sync Losses         1842953
Sig Losses          35246
Time at 0 Tx Credit 0

```

perf.openTrunking.backPressure

Syntax `backPressure backPressureState`

Purpose This command configures the Back Pressure state of the OpenTrunking configuration.

Parameters	This command has one parameter.
backPressureState	This parameter can be set to <i>enable</i> or <i>disable</i> OpenTrunking back pressure. Boolean 1 and 0 values may also be substituted. If the state is configured to be enabled, a back pressure entry is made to the Event Log and an SNMP trap is generated if SNMP is configured.

Command Example **Root>** perf openTrunking backPressure 1

perf.openTrunking.congestionThresh

Syntax	congestionThresh portNumber congestionThreshold
Purpose	This command configures the congestion threshold for an individual port or for all ports.
Parameters	This command has the following parameters.
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> applies the congestionThreshold value to every port on the product.
congestionThreshold	Specifies the congestion threshold in terms of a percentage. Valid values are integers in the range 1 to 99 or <i>default</i> . Specifying the value <i>default</i> sets the specified port to the default threshold level of 10.

Command Example **Root>** perf openTrunking congestionThresh 8 20

perf.openTrunking.lowBBCreditThresh

Syntax	lowBBCreditThresh lowBBCreditThreshold
Purpose	This command configures the low BB_credit threshold of the OpenTrunking configuration. The low BB_credit threshold is defined

as the percentage of time that no transmit BB_Credits are passed on the link. When the threshold value is exceeded, the system tries to reroute the flows that are going to the ISL with the problem. Effectively, the threshold is the percent of the time that the port does not receive BB_Credits before traffic is rerouted away from the port.

This threshold is also used for prevention of improperly rerouting to an ISL that lacks BB_Credits. In other words, the system does not reroute a flow to a link that lacks BB_Credits even if that link is significantly under its loading threshold. The system tries to reroute traffic away from a link that lacks BB_Credits, even if the loading threshold is significantly below the limit.

Parameters This command has one parameter.

lowBBCreditThreshold	Specifies the low BB_credit threshold in terms of a percentage. Valid values are integers in the range 1 to 99 or <i>default</i> . Specifying the value <i>default</i> sets the parameter to the default threshold level of 10%.
----------------------	--

Command Example **Root>** perf openTrunking lowBBCreditThresh 20

perf.openTrunking.setState

Syntax setState openTrunkingState

Purpose This command sets the enabled state of the OpenTrunking feature. The OpenTrunking feature key must be installed in order to enable open trunking.

Parameters This command has one parameter.

openTrunkingState	This parameter can be set to <i>enable</i> or <i>disable</i> the OpenTrunking feature. Boolean 1 and 0 may be substituted as values.
-------------------	--

Command Example **Root>** perf opentrunking setState 1

NOTE: The command [config.features.openTrunking](#) on page 2-8 has functionality that is identical to this command.

perf.openTrunking.show

Syntax `show portNumber`

Purpose This command displays the current OpenTrunking configuration per port.

Parameters This command has one parameter.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
------------	---

Command Example `Root> perf openTrunking show 11`

Output The OpenTrunking configuration data is displayed as a table that includes the following statistics.

Congestion Threshold	The threshold listed as a percentage. If the value is a default value, (default) is displayed next to the percentage.
Flows Rerouted To	Trunking statistic displaying flows rerouted to the specified port. (These statistics are cleared by the perf.clearStats command.)
Flows Rerouted From	Trunking statistic displaying flows rerouted from the specified port. (These statistics are cleared by the perf.clearStats command.)
Unresolved Congestion	The current enabled / disabled state of the unresolved congestion trunking feature. (The indicated state applies to every port on the product.)

Backpressure	The current enabled/disabled state of the backpressure trunking feature. (The indicated state applies to every port on the product.)
Low BB Credit Threshold	The current threshold setting of the Low BB Credit Threshold trunking feature. If the value is a default value, (default) is displayed next to the percentage. (The indicated value applies to every port on the product.)

Output Example The output from the `perf.openTrunking.show` command displays as follows.

```

Port Number:                1
Congestion Threshold (%):   56
Flows Rerouted To:         26739
Flows Rerouted From:       23987
Unresolved Congestion:     Enabled
Backpressure:               Disabled
Low BB Credit Threshold (%): 75 (default)

```

perf.openTrunking.unresCongestion

Syntax `unresCongestion unresolvedCongestionState`

Purpose This command configures the Unresolved Congestion state of the OpenTrunking configuration. If the state is configured to be enabled, an unresolved congestion entry is made to the Event Log and an SNMP trap is generated if SNMP is configured.

Parameters This command has one parameter.

`unresolvedCongestionState` This parameter can be set to *enable* or *disable* the Unresolved Congestion state of the OpenTrunking configuration. Boolean 1 and 0 values may also be substituted.

Command Example `Root> perf openTrunking unresCongestion 1`

perf.preferredPath

The perf.preferredPath commands enable you to use the Preferred Path feature to influence the route of data traffic that traverses multiple switches or directors in a fabric. If more than one ISL connects switches in your SAN, this feature is useful for specifying an ISL preference for a particular flow.

The Preferred Path feature allows the user to enhance the system's path selection algorithm by providing the ability to prioritize ISLs for a selected port on the switch. The Preferred Path capability customizes the static load-balancing function by allowing the user to specify an ISL preference for each remote domain. Preferred Path, however, is still subject to the standard Fabric Shortest Path First (FSPF) requirements, which allow the firmware to override the configuration setting if errors are encountered.

The data path consists of the source port of the switch or director being configured, the exit port of that switch or director, and the domain ID of the destination switch or director. Each switch or director must be configured for its part of the desired path in order to achieve optimal performance. You may need to configure Preferred Paths for all switches or directors along the desired path for a proper multi-hop Preferred Path. (For examples of Preferred Path implementation and other related information, see your product's Element Manager manual.)

The following rules apply when configuring Preferred Paths:

- The switch's domain ID must be set to insistent.
- Domain IDs must be in the range of 1 through 31.
- The specified numbers for source ports and exit ports must be in the range equal to the number of ports for the switch being configured.
- For any source port, only one path may be defined to each destination domain ID.

perf.preferredPath.clearPath

Syntax `clearPath destDomainID sourcePort`

Purpose This command deletes a preferred path. The command causes the specified path to use a path selection algorithm that is different from

the preferred path. All configured paths can be removed by specifying the *all* parameter for both the destination domain ID and source port.

Parameters This command has the following parameters.

destDomainId	Specifies the destination domain ID. Valid domain IDs are in the range 1–31 or <i>all</i> , which deletes all preferred paths to and from the source port specified in the sourcePort parameter.
sourcePort	Specifies the number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or you can specify <i>all</i> to delete all paths to the destination domain ID.

Command Example **Root>** perf preferredPath clearPath 10 5

perf.preferredPath.setPath

Syntax setPath destDomainID sourcePort exitPort

Purpose This command sets a preferred exit port given the destination domain ID and source port. An exit port can be set for each combination of destination domain ID and source port.

NOTE: You cannot set a path where the Destination Domain ID is the same as the Switch's Domain ID.

Parameters

This command has the following parameters.

destDomainId	Specifies the destination domain ID. Valid domain IDs are in the range 1–31.
sourcePort	Specifies the number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
exitPort	Specifies the number of the desired exit port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140

Command Example

```
Root> perf preferredPath setPath 17 5 11
```

perf.preferredPath.setState

Syntax `setState enabledState`

Purpose This command enables or disables the Preferred Path feature.

NOTE: Insistent domain IDs must be used in order to enable the preferred path state.

Parameters	This command has one parameter.	
	enabledState	Sets the state of the preferred path feature. When disabled, the preferred path settings are ignored for all path selection decisions. Accepted values for this command are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 may be substituted as values.

Command Example **Root>** perf preferredPath setState enable

perf.preferredPath.showPath

Syntax showPath destDomainID sourcePort

Purpose This command displays the requested Preferred Path configuration. The output shows the configured preferred exit port. Using *all* for either the destination domain ID or the specified source Port parameter results in output that shows all configured and actual exit ports for the other parameter. If the destination domain is set to *all*, then all paths from the specified source port are displayed. If the source port is set to *all*, the output shows all source port paths to the specified domain. You cannot specify *all* for both of those parameters.

Parameters

This command has the following parameters.

destDomainId	Specifies the destination domain ID. Valid domain IDs are in the range 1–31 or <i>all</i> , which shows all paths to and from the source port specified in the sourcePort parameter.
sourcePort	Specifies the number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or, you can specify <i>all</i> to show all paths to the destination domain ID specified for the destDomainId parameter.

Output

The output from perf.preferredPath.showPath includes the following parameters.

Destination Domain	The destination domain ID for which a preferred path has been configured. This is displayed only if the destination domain parameter is set to <i>all</i> .
Source Port	This is the source port for which a preferred path to the specified destination domain ID is specified. This is displayed only if the source port parameter is set to <i>all</i> .
Preferred Exit Port	The configured Preferred Path exit port. This value can be any port number, or blank to indicate that no Preferred Path has been configured.

Command and Output Examples

The following examples show the output returned by the three methods of specifying the perf.preferredPath.showPath command.

Single values for both parameters

```
Root> perf preferredPath showPath 21 10
Preferred Path State: Enabled
Preferred Exit Port: Not Configured
```

destDomainId set to all

```
Root> perf preferredPath showPath all 15
Preferred Path State: Enabled
Destination Domain Preferred Exit Port
-----
1 23
3 24
4 23
17 12
```

sourcePort set to all

```
Root> perf preferredPath showPath 1 all
Preferred Path State: Enabled
Source Port Preferred Exit Port
-----
0 2
2 5
3 17
22 5
```

perf.preferredPath.showState

Syntax showState

Purpose This command shows the enablement state for Preferred Path

Parameters This command has no parameters.

Command Example Root> Perf PreferredPath showState

Command Output The output from this command displays the current state of the Preferred Path.

```
Preferred Path State: Disabled
```

perf.thresholdAlerts

The perf.thresholdAlerts commands enable you to configure alerts that notify you of specific conditions on your system.

You can configure a maximum of 16 threshold alerts, including both counter threshold alerts (CTAs) and throughput threshold alerts (TTAs). Each of these types of alerts have commands that are specific to the alert type.

- Counter threshold alerts: These are alerts that are triggered by counts of events. The commands used to configure these alerts start with “*perf.thresholdAlerts.counter*”.
- Throughput threshold alerts: These alerts are triggered by port throughput. The commands used to configure these alerts start with “*perf.thresholdAlerts.throughput*”.

For a list of the available threshold alerts counters, see [Alert Types and Counters](#) on page 2-118.

NOTE: The perf.thresholdAlerts commands are standard command line interface features. They do not require a feature key.

Creating Threshold Alerts

The tasks you need to complete to create and activate a threshold alert differ depending on the type of alert you are creating. To implement a counter threshold alert, see [Activating a Counter Threshold Alert](#), below. To implement a throughput alert, see [Activating a Throughput Threshold Alert](#) on page 2-117.

Activating a Counter Threshold Alert

In order to activate a counter threshold alert using the CLI, you must enter certain commands in order. Enable the threshold alert using the following order:

1. Create a counter threshold alert using the command [perf.thresholdAlerts.counter.addAlert](#) on page 2-120. Use this command to create a name for the threshold alert that you can use in subsequent commands. The threshold alert must then be configured using the other counter threshold alert commands.
2. Assign the threshold alert to a port using the command [perf.thresholdAlerts.counter.addPort](#) on page 2-121.

3. Configure the threshold alert using other `perf.thresholdAlert` commands. For example, you may want to associate the threshold alert counter with the threshold alert name using the [`perf.thresholdAlerts.counter.setCounter`](#) command, described on 2-123. Use the following commands to view alert settings and configure an alert:
 - [`perf.thresholdAlerts.counter.removePort`](#) on page 2-122
 - [`perf.thresholdAlerts.counter.setCounter`](#) on page 2-123
 - [`perf.thresholdAlerts.counter.setParams`](#) on page 2-124
 - [`perf.thresholdAlerts.counter.show`](#) on page 2-125
 - [`perf.thresholdAlerts.counter.showStatisticTable`](#) on page 2-126
4. Once the alert is fully configured, it can be activated using the [`perf.thresholdAlerts.setState`](#) command, described on 2-127. An alert cannot be modified unless it is in the disabled state.

Activating a Throughput Threshold Alert

In order to activate a throughput threshold alert using the CLI, you must enter certain commands in order. Enable the threshold alert using the following order:

1. Create a throughput threshold alert using the command [`perf.thresholdAlerts.throughput.addAlert`](#) on page 2-129. Use this command to create a name for the threshold alert that you can use in subsequent commands. The threshold alert must then be configured using the other throughput threshold alert commands.
2. Assign the threshold alert to a port using the command [`perf.thresholdAlerts.throughput.addPort`](#) on page 2-130.
3. Identify the throughput statistic that triggers the throughput threshold alert using the command [`perf.thresholdAlerts.throughput.setUtilType`](#) on page 2-132.
4. Identify the percentage of throughput that triggers the throughput threshold alert using the command [`perf.thresholdAlerts.throughput.setUtilPercentage`](#) on page 2-133.

5. Configure the threshold alert using other `perf.thresholdalert` commands. For example, you may want to set the duration and interval times for the alert, as described in [perf.thresholdAlerts.throughput.setParams](#) on page 2-134. Use the following commands to view alert settings and configure an alert:
 - [perf.thresholdAlerts.throughput.removePort](#) on page 2-131
 - [perf.thresholdAlerts.throughput.setParams](#) on page 2-134
 - [perf.thresholdAlerts.throughput.show](#) on page 2-135
 - [perf.thresholdAlerts.throughput.showUtilTypeTable](#) on page 2-135
6. Once the alert is fully configured, it can be activated using the [perf.thresholdAlerts.setState](#) command, described on 2-127. An alert cannot be modified unless it is in the disabled state.

Alert Types and Counters

[Table 2-2](#) provides a list of throughput threshold alerts.

Table 2-2 Throughput Threshold Alerts

Utilization Code	Threshold Alert Type
Tx Util	TTA - Transmit Utilization
Rx Util	TTA - Receive Utilization
Tx/Rx Util	TTA - Transmit or Receive Utilization

[Table 2-3](#) provides a list of threshold alert counters and counter sets.

Table 2-3 Alert Counters

Number	Threshold Alert Counter or Counter Set
1	Link Resets Sent
2	Link Resets Received
3	OLS Sent
4	OLS Received
5	Link Failures

Table 2-3 Alert Counters (Continued)

Number	Threshold Alert Counter or Counter Set
6	Sync Losses
7	Signal Losses
8	Protocol Errors
9	Invalid Tx Words
10	CRC Errors
11	Discarded Frames
12	Frames Too Short
13	Delimiter Errors
14	Address ID Errors
15	Class2BusiedFrames
16	Class2RejectedFrames
17	Class3DiscardedFrames
18	Physical Link Errors Set (see below)
19	Link Sequence Counts Set (see below)
20	Logical Link Errors Set (see below)
21	LIPS Detected (Sphereon 4300 and Sphereon 4500 switches only)
22	LIPS Generated (Sphereon 4300 and Sphereon 4500 switches only)

Description of Summed Sets

Some of the threshold alerts consist of groups of related items called *Summed Sets*. When any of the items in the summed set are encountered, the total value of the summed set counter is incremented. The items that make up the summed sets are:

- **Physical Link Errors Summed Set**
 - Link Failures
 - Sync Losses
 - Signal Losses
 - Protocol Errors
 - Invalid Tx Words
 - CRC Errors
 - Frames Too Short
 - Delimiter Errors
- **Link Sequence Counts Summed Set**
 - Link Resets Received
 - Link Reset Sent
 - OLS Received
 - OLS Sent
- **Logical Link Errors Summed Set**
 - Discarded Frames
 - Address ID Errors
 - Class 2 Busied Frames
 - Class 2 Rejected Frames
 - Class 3 Discarded Frames

perf.thresholdAlerts.counter.addAlert

Syntax addAlert name

Purpose This command configures a new counter threshold alert and assigns it a name. The new alert is assigned default settings which can then be changed using the other counter threshold alert commands.

The default settings for a new counter threshold alert are as follows:

- Ports: None
- Counter: None
- Increment: 100

- Interval: 60 minutes
- State: Disabled

Parameters This command has one parameter.

name	Specifies the name of the new counter threshold alert. This name can consist of any ASCII characters up to a maximum length of 64 characters. To use spaces or special characters in this name, put quotation marks around the name. This parameter is case-sensitive.
------	--

TIP: Although the system supports a name length of 64 characters, you may want to use a much shorter name. Some commands that display the threshold name show a maximum of 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the `commaDelim` command. For more information, see [Using the commaDelim Command](#) on page 1-17.

Command Example **Root>** perf thresholdAlerts counter addAlert checklinks

perf.thresholdAlerts.counter.addPort

Syntax `addPort name portNumber`

Purpose This command adds a port to the specified counter threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters.

name	The name of a counter threshold alert as defined by the command perf.thresholdAlerts.counter.addAlert on page 2-120.
portNumber	Specifies the port number or port type. Valid port number values: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> applies the counter threshold alert to every port on the product.

Specifying a port type removes all the ports from the alert and applies the alert to each port that is the specified type of port. Valid values are:

- *eport*
- *fport*
- *flport* (Sphereon 4300 and Sphereon 4500 only)

NOTE: A counter threshold alert is not allowed to specify both port types and individual port numbers.

Command Example

```
Root> perf thresholdAlerts counter addPort checklinks 12
```

perf.thresholdAlerts.counter.removePort**Syntax**

```
removePort name portNumber
```

Purpose

This command removes a port from the specified counter threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters.

name	The name of a counter threshold alert as defined by the command perf.thresholdAlerts.counter.addAlert , described on 2-120.
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> removes every port on the product from the counter threshold alert.

Command Example

Root> perf thresholdAlerts counter removePort checklinks 12

perf.thresholdAlerts.counter.setCounter

Syntax setCounter name counterNumber

Purpose This command sets the counter statistic that will be used to trigger the counter threshold alert. Use this command to associate a counter with the threshold alert name created using the [perf.thresholdAlerts.counter.addAlert](#) command.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters.

name	The name of a counter threshold alert as defined by the command perf.thresholdAlerts.counter.addAlert , described on 2-120.
counterNumber	Specifies the counter number. Valid values are shown in Table 2-3, Alert Counters , page 2-118.

Command Example

```
Root> perf thresholdAlerts counter setCounter checklinks 1
```

perf.thresholdAlerts.counter.setParams**Syntax**

```
setParams name increment interval
```

Purpose

This command sets the increment and interval times for a specified counter threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters.

name	The name of a counter threshold alert as defined by the command perf.thresholdAlerts.counter.addAlert , described on 2-120.
increment	This sets the number of times a counter must increment during the interval period to trigger the alert. Acceptable values are in the range of 1 to 70,560.
interval	This sets the interval time in minutes for the alert. Acceptable values are in the range of 5 to 70,560 minutes.

Example

The meaning for each of these inputs can best be described using the following example sentence:

If ports 0,1, or 2 CRC Error counter increments more than 5 times within a period of 30 minutes, send an alert. Where:

```
Port list      = 0, 1, 2
CTA Counter    = CRCErrors
Increment value = 5
Interval Time  = 30
```

The increment value takes place in an interval that is a fixed length amount of time. This interval is not a rolling window interval.

Command Example **Root>** perf thresholdAlerts counter setParams checklinks 5 30

perf.thresholdAlerts.counter.show

Syntax show name

Purpose This command displays the settings for an individual counter threshold alert.

Parameters This command has one parameter.

name	The name of a threshold alert as defined by the command perf.thresholdAlerts.counter.addAlert , described on 2-120. You can specify <i>all</i> instead of a name, which means that all threshold alerts are displayed.
------	---

NOTE: The output of this command truncates threshold alert names that are longer than 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the commaDelim command. For more information, see [Using the commaDelim Command](#) on page 1-17.

Command Example **Root>** perf thresholdAlerts counter show checklinks

Output Example The output from the perf.thresholdAlerts.counter.show command displays as follows.

```
Index:          3
Name:           Example_CRC_Error_Finder
Ports:          2,4-7,20-24
Counter Statistic: CRC Errors
Increment:      5
```

Interval: 30
Alert State: Disabled

perf.threshholdAlerts.counter.showStatisticTable

Syntax showStatisticTable

Purpose This command displays the table of different statistic counters that can be added to a counter threshold alert. This table is used for reference only.

This command has no parameters.

Command Example **Root>** perf threshAlerts counter showStatisticTable

Output Example The output from the perf.threshholdAlerts.counter.showStatisticTable command displays as follows.

Number	Counter or Counter Set
-----	-----
1	Link Resets Sent
2	Link Resets Received
3	OLS Sent
4	OLS Received
5	Link Failures
6	Sync Losses
7	Signal Losses
8	Protocol Errors
9	Invalid Tx Words
10	CRC Errors
11	Discarded Frames
12	Frames Too Short
13	Delimiter Errors
14	Address ID Errors
15	Cls2 BusiedFrms
16	Cls2 RejectedFrms
17	Cls3 DiscardFrms
18	Phys Lnk Err Set
19	Lnk Seq Cnt Set
20	Logic Lnk Err Set
21	LIPS Detected
22	LIPS Generated

perf.thresholdAlerts.deleteAlert

Syntax `deleteAlert name`

Purpose This command deletes a specified threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters This command has one parameter.

name	The name of a threshold alert as defined by the commands perf.thresholdAlerts.counter.addAlert and perf.thresholdAlerts.throughput.addAlert , or, enter <i>all</i> to delete all of the configured threshold alerts.
------	--

Command Example **Root>** `perf thresholdAlerts deleteAlert checklinks`

perf.thresholdAlerts.setState

Syntax `setState name enabledState`

Purpose This command sets the enabled state of the specified threshold alert.

Parameters This command has the following parameters.

name	The name of a threshold alert as defined by the commands perf.thresholdAlerts.counter.addAlert and perf.thresholdAlerts.throughput.addAlert .
enabledState	Sets the counter threshold alert enabled state. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 values may also be substituted.

Command Example **Root>** `perf thresholdAlerts setState checklinks enabled`

perf.thresholdAlerts.show

Syntax `show`

Purpose This command displays information about all threshold alerts.

Parameters This command has no parameters.

Command Example **Root>** perf thresholdAlerts show

Output The data is displayed as a table that includes the following properties:

Name	The name of the threshold alert (truncated to 51 characters).
Type	The trigger statistic or threshold type of the alert (abbreviated to 17 chars).
Tx Util	TTA - Transmit Utilization
Rx Util	TTA - Receive Utilization
Tx/Rx Util	TTA - Transmit or Receive Utilization
Link Resets Sent	CTA - Link Resets Sent
Link Resets Received	CTA - Link Resets Received
OLS Sent	CTA - OLS Sent
OLS Received	CTA - OLS Received
Link Failures	CTA - Link Failures
Sync Losses	CTA - Sync Losses
Signal Losses	CTA - Signal Losses
Protocol Errors	CTA - Primitive Sequence Errors/Protocol Errors
Invalid Tx Words	CTA - Invalid Tx Words
CRC Errors	CTA - CRC Errors
Discarded Frames	CTA - Discarded Frames
Frames Too Short	CTA - Frames Too Short
Delimiter Errors	CTA - Delimiter Errors

Address ID Errors	CTA - Address ID Errors
Cls2 BusiedFrms	CTA - Class 2 Busied Frames
Cls2 RejectedFrms	CTA - Class 2 Rejected Frames
Cls3 DiscardFrms	CTA - Class 3 Discarded Frames
Phys Lnk Err Set	CTA - Physical Link Errors Summed Set
Lnk Seq Cnt Set	CTA - Link Sequence Counts Summed Set
Logic Lnk Err Set	CTA - Logical Link Errors Summed Set
LIPs Detected	CTA - Loop Initialization Primitive Detected
LIPs Generated	CTA - Loop Initialization Primitive Generated

State The enabled state of the CTA. Either enabled or disabled.

Output Example

Name	Type	State
-----	-----	-----
Throughput Threshold #1	Rx Util	Enable
Threshold for CRC	CRC Errors	Disabled
Safety #2	Logic Lnk Err Set	Enabled
Safety #1	Cls2 BusiedFrms	Disabled

perf.thresholdAlerts.throughput.addAlert

Syntax addAlert name

Purpose This command configures a new throughput threshold alert and assigns it a name. The new alert is assigned default settings that can then be changed using the other throughput threshold alert commands.

 The default settings for a new counter threshold alert are as follows:

- Ports: None
- Utilization Type: None
- Utilization Percentage: 50%
- Duration: 30 minutes
- Interval: 60 minutes
- Alert State: Disabled

Parameters This command has the following parameter.

name	Specifies the name of the new throughput threshold alert. This name can consist of any ASCII characters up to a maximum length of 64 characters. To use spaces or special characters in this name, put quotation marks around the name. This parameter is case-sensitive.
------	---

TIP: Although the system supports a name length of 64 characters, you may want to use a much shorter name. Some commands that display the threshold name show a maximum of 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the `commaDelim` command. For more information, see [Using the commaDelim Command](#) on page 1-17.

Command Example `Root> perf thresholdAlerts throughput addAlert port6Rx`

perf.thresholdAlerts.throughput.addPort

Syntax `addPort name portNumber`

Purpose This command adds a port to the specified throughput threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters This command has the following parameters.

name	The name of a throughput threshold alert as defined by the command <i>perf.thresholdAlerts.throughput.addAlert</i> , described on 2-129.
portNumber	Specifies the port number or port type. Valid values are either a single port number, all ports, or port type. The following port numbers are valid: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> applies the throughput threshold alert to every port on the product.

Specifying a **port type** removes the alert from all ports and applies the alert to all ports of the specified type. Valid values are:

- *eport*
- *fport*
- *flport* (Sphereon 4300 and Sphereon 4500 only)

NOTE: This parameter cannot specify both individual port numbers and a port type.

Command Example `Root> perf thresholdAlerts throughput addPort eportRx eport`

perf.thresholdAlerts.throughput.removePort

Syntax `removePort name portNumber`

Purpose This command removes a port from the specified throughput threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters

This command has the following parameters.

name	The name of a throughput threshold alert as defined by the command perf.thresholdAlerts.throughput.addAlert , described on 2-129.
portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> removes the throughput threshold alert from every port on the product.

Command Example

Root> perf thresholdAlerts throughput removePort eportRx all

perf.thresholdAlerts.throughput.setUtilType**Syntax**

setUtilType name utilizationType

Purpose

This command sets the throughput statistic that is used to trigger the throughput threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters	This command has the following parameters.	
	name	The name of a throughput threshold alert as defined by the command perf.thresholdAlerts.throughput.addAlert , described on 2-129.
	utilizationType	The type of traffic that triggers the alert. Enter the number that corresponds to the desired utilization type: 1 - Transmit Traffic (Tx) 2 - Receive Traffic (Rx) 3 - Both (Rx and Tx)

Command Example **Root>** perf thresholdAlerts throughput setUtilType eportRx 1

perf.thresholdAlerts.throughput.setUtilPercentage

Syntax setUtilPercentage name utilizationPercentage

Purpose This command sets the throughput utilization percentage that is used to trigger the throughput threshold alert.

NOTE: An alert cannot be modified unless it is in the disabled state. Verify that the alert is disabled before executing this command.

Parameters	This command has the following parameters.	
	name	The name of a throughput threshold alert as defined by the command perf.thresholdAlerts.throughput.addAlert , described on 2-129.
	utilizationPercentage	The percentage of throughput utilization that triggers the alert. This must be entered as a number. Accepted values are in the range 1 to 100.

Command Example **Root>** perf thresholdAlerts throughput setUtilPercentage eportRx 70

perf.thresholdAlerts.throughput.setParams

Syntax `setParams name duration interval`

Purpose This command sets the duration and interval times for a specified throughput threshold alert. This command enables you to configure the alert to be sent if both of the following events occur:

- The throughput threshold alert value is surpassed for more than the timespan specified for the duration parameter.
- The duration parameter is surpassed within the time frame specified by the interval parameter.

Parameters This command has the following parameters.

name	The name of a throughput threshold alert as defined by the command perf.thresholdAlerts.throughput.addAlert , described on 2-129.
duration	The duration time in minutes that the utilization must exist to trigger the alert. Acceptable values are in the range 0 to 70,560 minutes. Setting this value to zero means that the alert is triggered if the specified utilization is exceeded at any time. The value of this parameter must be less than or equal to the value of the interval parameter.
interval	This sets the interval time in minutes. The interval is a fixed length of time. It is not a rolling window of time. Acceptable values are in the range 5 to 70,560 minutes. The value of this parameter must be greater than or equal to the value of the duration parameter.

Command Example

```
Root> perf thresholdAlerts throughput SetParams eportRx 1  
10
```

perf.thresholdAlerts.throughput.show

Syntax `show name`

Purpose This command displays the settings for an individual throughput threshold alert.

Parameters This command has the following parameter.

name	The name of a throughput threshold alert as defined by the command perf.thresholdAlerts.throughput.addAlert , described on 2-129. You can specify <i>all</i> instead of a name, which means that all threshold alerts are displayed.
------	---

NOTE: The output of this command truncates threshold alert names that are longer than 51 characters. If you specify lengthy names, you can display the complete name by entering the comma-delimited mode using the `commaDelim` command. For more information, see [Using the commaDelim Command](#) on page 1-17.

Command Example `Root> perf thresholdAlerts throughput show eportRx`

Output Example The output from the `perf.thresholdAlerts.throughput.show` command displays as follows.

```
Name:                      90% Receive Throughput Threshold
Ports:                     5,8,12,20-24
Utilization Type:          Rx
Utilization Percentage:    90%
Duration:                  15
Interval:                  30
Alert State:               Disabled
```

perf.thresholdAlerts.throughput.showUtilTypeTable

Syntax `showUtilTypeTable`

Purpose This command displays a table of the utilization types that can be used for a throughput threshold alert. This table is used for reference only.

Parameters This command has no parameters.

Command Example **Root>** perf thresholdAlerts throughput showUtilTypeTable

Output Example The output from the perf.thresholdAlerts.throughput.showUtilTypeTable command displays as follows.

Number	Utilization Type
1	Transmit Traffic (Tx)
2	Receive Traffic (Rx)
3	Both (Tx/Rx)

perf.traffic

Syntax traffic portNumber

Purpose This command displays port traffic counters for a specified port.

Parameters This command has one parameter.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
------------	---

Command Example **Root>** perf traffic 2

Output The port traffic counter data is displayed as a table that includes the following statistics, along with a wrap count for each corresponding counter.

Port	The port number.
Rx%	The received link utilization percentage.
Tx%	The transmitted link utilization percentage.
RxFrames	The number of Fibre Channel Class 2 and Class 3 frames that the port has received.

TxFrames	The number of Fibre Channel Class 2 and Class 3 frames that the port has transmitted.
RxWords	The number of 4-byte words in Class 2 and Class 3 frames that the port has received.
TxWords	The number of 4-byte words in Class 2 and Class 3 frames that the port has transmitted.

Output Example The output from the perf.traffic command displays as follows.

Port 2		
Statistic	Wrap	Count
-----	-----	-----
Rx%	N/A	75
Tx%	N/A	30
RxFrames	23	2953184
TxFrames	12	1842953
RxWords	65	2953184
TxWords	32	1842953

show

The show branch of the CLI command tree contains commands that display, but do not change, stored data values. The displayed output that results from these commands is not necessarily identical with the output from the show commands that are within the other CLI command tree branches, for example, config.port.show.

The commands in the show branch can be used by either the administrator or the operator.

show.all

Syntax all

Purpose This command displays all configuration and status information available. The command results in a sequential display of the output of other CLI show commands. This set of show commands returns the full configuration and status of the switch and fabric.

Parameters This command has no parameters.

Command Example **Root>** show all

Output The output of this command is a sequential display of the output of other CLI show commands. The commands are displayed in the following order:

- show.ip.ethernet
- show.system
- show.switch
- show.port.config
- show.frus
- config.snmp.show
- show.zoning
- show.port.state
- show.port.info
- show.port.technology
- show.loginserver

- show.features
- show.security.portbinding
- show.security.switchbinding
- show.security.fabricbinding
- show.openTrunking.config
- show.thresholdAlerts.alerts
- show.fabric.topology
- show.fabric.nodes
- show.security.switchACL
- show.ficonCUPZoning
- show.FencingPolicies

show.auditLog

Syntax auditLog [clear]

Purpose This command displays the entries of the audit log after the last time the log was cleared.

Parameters This command has one optional parameter.

clear	Adding the optional 'clear' parameter removes all entries from the log. If the log is full, it will resume collecting log entries.
-------	--

Command Example show auditLog

Output The output from this command displays the following data.

Date/Time	The date and time of the log entry.
Action	Type of Audit Log event.
Source	Source of Audit Log event.
User ID	Identifier of the user that made the command. Usually an IP Address.

Output Example

Date/Time	Action	Source	User Id
-----	-----	-----	-----
11/24/03 04:18P	Switch set online	CLI	172.16.22.23
11/24/03 03:38P	Switch name modified	CLI	172.16.22.23
11/24/03 03:38P	Switch set offline	CLI	172.16.22.23
11/24/03 11:27A	Firmware downloaded	Web	172.60.5.40

show.epFrameLog.config**Syntax** config**Purpose** This command shows the current Embedded Frame Log settings**Parameters** This command has no parameters.**Command Example** **Root>** show epFrameLog config**Output** The output from this command displays the following data.

Filter Class F Frames	The state for filtering of Class F frames.
Filter Port	The port that is being filtered on.

Output Example

Filter Class F Frames:	Disabled
Filter Port:	All

show.epFrameLog.filterClassFFrames**Syntax** filterClassFFrames [enable]**Purpose** This command will turn on or off the ability to filter out class-F frames, or show its current state. When the filtering is enabled, everything but class-F frames will be logged. This setting will not be stored in NV RAM and will not persist after IML.

Parameters This command has one optional parameter. If no parameters are entered, it will show the current state.

enable	Specifies the on/off state. Valid values are <i>enable</i> and <i>disable</i> . Boolean 1 and 0 values may also be substituted.
--------	---

Command Example **Root>** show epFrameLog filterClassFFrames enable

show.epFrameLog.setFilterPort

Syntax setFilterPort portNumber

Purpose This command sets the port number that the Embedded Port Frame Log will use for logging. Only frames from the port number that is set will be added to the log.

Parameters This command has one parameter.

portNumber	This parameter can be set to any port number (except inaccessible and unaddressable ports), <i>all</i> , or <i>none</i> .
------------	---

Command Example **Root>** show epFrameLog setFilterPort 63

Parameters This command has one optional parameter. If no parameters are entered, it will show the current state.

newPort	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 <i>all</i> - make the FC2 log collect entries from all of the posts on the switch. <i>none</i> - make the FC2 log stop collecting entries.
---------	--

Command Example **Root>** show epFrameLog setFrameLogPort 63

show.epFrameLog.noWrap

Syntax noWrap [clear]

Purpose This command allows the user to view the contents of the non-wrapping region of the FC2 frame log. The log entries will not persist IMLs or power cycles; it will not be stored in NV RAM. This log will not include entries for frames discarded by hardware, such as un-routable class-3 frames unless class-3 discard is disabled in the hardware.

NOTE: This log will not wrap. The log will stop collecting entries after it is filled.

Parameters This command has one optional parameter. If no parameter is specified, then the 500 entries of the log will be displayed.

clear	Adding the optional 'clear' parameter removes all entries from the log.
-------	---

Command Example show epFrameLog noWrap

Output This command displays the following data.

Count	A constantly incrementing counter.
Date/Time	Time of the frame.
Port #	The port number.
Direction	Direction of the frame through the port (I = In, O = Out).
SOF	Start of frame.
EOF	End of frame.
Header	The 24 byte FC frame header.
PL (size in bytes)	The first 32 bytes of the FC frame payload.

Output Example

The output of the `show.epFrameLog.nowrap` command displays as follows:

Count	Date/Time	Port #	Direction	SOF	EOF	Payload Size
39	11/24/03 11:30A	39	O	i3	n	2112
Header:	22000026 000000EF	E1000000	00000000	FFFF0000	00000000	
PL:	00010203 04050607	08090A0B	0C0D0E0F	10111213	14151617	18191A1B 1C1D1E1F
38	11/24/03 11:30A	38	I	i3	n	2112
Header:	22000026 000000EF	E1000000	00000000	FFFF0000	00000000	
PL:	00010203 04050607	08090A0B	0C0D0E0F	10111213	14151617	18191A1B 1C1D1E1F
37	11/24/03 11:30A	38	O	i3	n	2112
Header:	22000025 000000EF	E1000000	00000000	FFFF0000	00000000	
PL:	00010203 04050607	08090A0B	0C0D0E0F	10111213	14151617	18191A1B 1C1D1E1F

show.epFrameLog.wrap

Syntax `wrap [clear]`

Purpose This command allows the user to view the contents of the wrapping region of the FC2 frame log. The log entries will not persist IMLs or power cycles, and will not be stored in NV RAM. This log will not include entries for frames discarded by hardware, such as un-routable class-3 frames unless class-3 discard is disabled in the hardware.

NOTE: This log will begin to wrap after the log is filled.

Parameters This command has one optional parameter. If no parameter is specified, then the 1000 entries of the log will be displayed.

`clear` Adding the optional 'clear' parameter removes all entries from the log.

Command Example `Root> show epFrameLog wrap`

Output This command displays the following data.

Count	A constantly incrementing counter.
Date/Time	Time of the frame.
Port #	The port number.

Direction	Direction of the frame through the port (I = In, O = Out).
SOF	Start of frame.
EOF	End of frame.
Header	The 24 byte FC frame header.
PL (size in bytes)	The first 32 bytes of the FC frame payload.

Output Example

The output of the show.epFrameLog.wrap command displays as follows:

Count	Date/Time	Port #	Direction	SOF	EOF	Payload Size
39	11/24/03 11:30A	39	O	i3	n	2112
Header: 22000026 000000EF E1000000 00000000 FFFF0000 00000000						
PL: 00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F						
38	11/24/03 11:30A	38	I	i3	n	2112
Header: 22000026 000000EF E1000000 00000000 FFFF0000 00000000						
PL: 00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F						
37	11/24/03 11:30A	38	O	i3	n	2112
Header: 22000025 000000EF E1000000 00000000 FFFF0000 00000000						
PL: 00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F						

show.eventLog

Syntax eventLog [clear]

Purpose This command shows the contents of the event log as maintained in NV-RAM on the director or switch.

Parameters This command has one parameter.

clear This optional parameter causes all event log entries to be cleared.

Command Example **Root>** show eventLog

Output The event log data are displayed as a table that includes the following properties.

Date/Time	The date and time when the event occurred.
Code	The event reason code.
Severity	The severity of the event. The values are: <ul style="list-style-type: none"> • Major—Unit operational (major failure). • Minor—Unit operational (minor failure). • Severe—Unit not operational. The causes are either that the switch contains no operational SBAR cards or that the system shuts down due to CTP thermal threshold violations. • Info—Unit operational (information only).
FRU	The FRU and FRU position, where applicable.
Event Data	The 32-byte hexadecimal description of the event in words.

Output Example The output from the show.eventLog command displays as follows.

Date/Time	Code	Severity	FRU	Event Data
04/12/01 10:58A	375	Major	CTP-0	00010203 04050607 08090A0B 0C0D0E0F
04/12/01 9:58A	385	Severe	CTP-0	00010203 04050607 08090A0B 0C0D0E0F
04/11/01 7:18P	395	Severe	CTP-0	00010203 04050607 08090A0B 0C0D0E0F

show.fabricLog.noWrap

Syntax noWrap [clear]

Purpose This command allows the user to view the contents of the non-wrapping region of the fabric log. The log entries will not persist IMLs or power cycles; it will not be stored in NV RAM.

NOTE: This log will not wrap. The log will stop collecting entries after it is filled.

Parameters This command has one optional parameter. If no parameter is specified, then the 200 entries of the log will be displayed.

clear Removes all entries from the log.

Command Example `show fabricLog noWrap`

Output This command displays the following data.

Count	A constantly incrementing counter.
Date/Time	The date and time of the log entry.
Description	A description of the log entry.
Data	Extended data that is associated to the log entry.

Output Example The output of the `show.fabricLog.noWrap` command displays as follows:

Count	Date/Time	Description
-----	-----	-----
11	11/24/03 04:18P	Port RSCN
Data: RSCN Reason=2301, Port Offline/Online=26437, Ports 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143,		
144		
10	12/04/03 08:15A	Fabric Operational
Data:		
9	12/04/03 08:15A	Paths Operational
Data:		
8	12/04/03 08:15A	Zone Merge Completed

show.fabricLog.wrap

Syntax `wrap [clear]`

Purpose This command allows the user to view the contents of the wrapping region of the fabric log. The log entries will not persist IMLs or power cycles; it will not be stored in NV RAM.

NOTE: This log will begin to wrap after the log is filled.

Parameters This command has one optional parameter. If no parameter is specified, then the 1000 entries of the log will be displayed.

clear Removes all entries from the log.

Command Example show fabricLog Wrap

Output This command displays the following data.

Count	A constantly incrementing counter.
Date/Time	The date and time of the log entry.
Description	A description of the log entry.
Data	Extended data that is associated to the log entry.

Output Example The output of the show.fabricLog.wrap command displays as follows:

Count	Date/Time	Description
-----	-----	-----
11	11/24/03 04:18P	Port RSCN
Data: RSCN Reason=2301, Port Offline/Online=26437, Ports 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 40, 41, 42, 43, 44, 45, 46, 47, 48, 49,50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143,		
144		
10	12/04/03 08:15A	Fabric Operational
Data:		
9	12/04/03 08:15A	Paths Operational
Data:		
8	12/04/03 08:15A	Zone Merge Completed
Data:		

show.fabric.nodes

Syntax nodes

Purpose This command displays a list of all fabric-attached nodes.

Parameters This command has no parameters.

Command Example **Root>** show fabric nodes

Output The data is displayed as a table that includes the following properties.

Domain ID	Domain ID of the switch to which the device is attached.
Node WWN	The WWN of the fabric attached node.

Output Example The output from the show.fabric.nodes command displays as follows.

Domain ID	Node WWN
2	12:34:7C:CC:57:86:37:23
2	98:45:75:25:7B:35:30:34
2	27:35:3E:69:63:34:22:11
2	29:81:24:74:57:32:48:98
6	25:F2:35:7A:25:22:11:0B
18	F1:23:96:43:56:A3:AA:12
18	45:4D:2B:22:62:9B:19:91

show.fabric.principal

Syntax principal

Purpose This command displays the WWN of the principal switch in the fabric.

Parameters This command has no parameters.

Command Example **Root>** show fabric principal

Output The data is displayed as a table that includes the following properties:

Principal Switch WWN	The WWN of the principal switch in the fabric.
----------------------	--

Output Example Principal Switch WWN: 00:00:00:00:00:00:00:00

show.fabric.topology

Syntax topology

Purpose This command displays a text description of the fabric. The principal switch in the fabric will have a "*" next to it.

Parameters This command has no parameters.

Command Example **Root>** show fabric topology

Output The features data is displayed as a table that includes the following properties.

Switch WWN	The WWN of the switch at the local end of the ISL.
DID	Domain ID of the switch at the local end of the ISL.
OutPrt	The port number at the local end of the ISL.
Remote WWN	The WWN of the switch at the remote end of the ISL.
RemDID	The domain ID of the switch at the remote end of the ISL.
RemPrt	The port number at the remote end of the ISL.

Output Example The output from the show.fabric.topology command displays as follows.

Switch WWN	DID	OutPrt	Remote WWN	RemDID	RemPrt
02:30:40:32:34:34:32:21*	2	24	24:45:73:49:05:43:22:11	10	2
		25	24:45:73:49:05:43:22:11	10	3
		26	24:45:73:49:05:43:22:11	10	4
24:45:73:49:05:43:22:11	10	2	02:30:40:32:34:34:32:21	2	24
		3	02:30:40:32:34:34:32:21	2	25
		4	02:30:40:32:34:34:32:21	2	26
21:23:21:25:76:43:23:21	10	7	02:30:40:32:34:34:32:21	15	3
02:30:40:32:34:34:32:21	15	3	21:23:21:25:76:43:23:21	10	7

show.features

Syntax `features`

Purpose This command displays a table of all installed feature sets and their states. This command provides the same output as the command [*config.features.show*](#) on page 2-9.

Parameters This command has no parameters.

Command Example **Root>** `show features`

Output The features data is displayed as a table that includes the following properties.

Installed Feature Set	The feature set installed using a feature key. Only installed keys are displayed.
Feature	Individual features within each set. In many cases, there is only one feature within each feature set.
State	The state of the individual feature. Fabric-wide features are displayed as Active/Inactive. Switch-centric features are displayed as Enabled/Disabled.

Output Example The output from the `show.features` command displays as follows.

Installed Feature Set	Feature	State
-----	-----	----
Open Systems Management Server	OSMS	Enabled
Flex Ports	8 Flex Ports	Enabled
SANtegrity	Fabric Binding	Active
SANtegrity	Switch Binding	Enabled
SANtegrity	Enterprise Fabrics	Active
Open Trunking	Open Trunking	Enabled

show.fencing.policies

Syntax `fencing [name]`

Purpose This command displays a table of the configured fencing policies. If a specific policy name is given, then a full description of the policy is shown.

Parameters This command has one optional parameter, an individual policy name. If an individual policy name is given, then a detailed description will be shown for the specified policy. If no parameter is given, then a summary of all policies will be shown.

Command Example

```
Root> show fencing
Root> show fencing Protocol Errors #2
```

Output The data is displayed as a table that includes the following properties:

Name	The name of the policy. This will be concatenated to 50 characters in the summary display. The policy full name will be shown in comma-delim mode.
Ports	The ports to which the fencing policy will be applied.
Type	The type of the fencing policy.
Limit	The number of offenses that are allowed before a port is disabled.
Period	The amount of time that limit of number of offenses must exceed before a port is fenced.
State	The enabled state of the fencing policy.

Output Example

```
Root> show fencing
Name                                     Type                                     State
-----
Default_Protocol_Errors                 Protocol Errors                         Enabled
Protocol Errors #2                      Protocol Errors                         Disabled
Safety #2                               Protocol Errors                         Enabled

Root> show fencing Protocol Errors #2
Name:                                     Protocol Errors #2
Ports:                                   2,4-7,20-24
Type:                                    Protocol Errors
Limit:                                    5
Period:                                 1800 seconds
State:                                   Disabled
```

show.ficonCUPZoning

Syntax `ficonCUPZoning`

Purpose This command displays the contents of the host control list and the enabled state of FICON CUP Zoning.

NOTE: The command [config.ficonCUPZoning.show](#) on page 2-18 has functionality that is the same as this command.

Parameters This command has no parameters.

Command Example `show ficonCUPzoning`

Output The data is presented as a table with the following properties:

FICON CUP Zoning State	The enabled state of the FICON CUP Zoning feature
Host Control List	List of 0-8 control hosts, displays "empty" for control host list with no members.

Output Example FICON CUP Zoning State: Enabled
Host Control List

01:02:03:04:05:06:07:08
09:0A:0B:0C:0D:0E:0F:00

show.ficonMS

Syntax `ficonMs`

Purpose This command show the Ficon MS settings

NOTE: This command is displayed on a Sphereon 3016 only if the feature key is installed.

Parameters This command has no parameters.

Command Example **Root>** `show ficonms`

Output The data is displayed as a table that includes the following properties:

Ficon MS State	The state of the Ficon MS feature.
Ficon MIHPTO	The Ficon MIHPTO value in seconds.

Output Example

```
Ficon MS State:           Disabled
Ficon MIHPTO (seconds):  180
```

show.frus

Syntax frus

Purpose This command displays information about all FRUs.

Parameters This command has no parameters.

Command Example **Root>** show frus

Output The FRU information is displayed as a table that includes the following properties.

FRU	The FRU name. (This may show <i>Unknown</i> or <i>Not Installed</i> , if the FRU is not installed.)
Position	The relative position of the FRU, that is, its slot.
State	The state of the FRU. Values are: Active—the current module is active. Backup—this module is not currently being used, but it is available for immediate failover. NotInst—the module is not currently installed. Failed—the current module is failed.
Serial Num	The serial number of the FRU. (This field is blank for power supply modules of the Sphereon 4300 and Sphereon 4500 switches.)
Part Num	The part number of the FRU.
Beacon	The beaconing state of the FRU (On or Off).
Pwr On Hrs	The power-on hours value for the FRU.

Output Example

The output from the show.frus command displays as follows.

FRU	Position	State	Serial Num	Part Num	Beacon	Pwr On Hrs
-----	-----	-----	-----	-----	-----	-----
CTP	0	Active	470-000399-700	123456789	Off	2800
CTP	1	Backup	470-000399-700	223456789	On	2801
SBAR	0	Active	470-000399-700	223456789	Off	2801
SBAR	1	Failed	470-000399-700	223456789	Off	2801
FPM	1	Active	470-000399-700	223456789	Off	2801
FPM	3	Active	470-000399-700	223456789	Off	831
UPM	4	Active	470-000399-700	223456789	Off	831
Power	0	Active	470-000399-700	223456789	Off	831
Fan	0	Active	470-000399-700	223456789	Off	831

show.ip.ethernet

Syntax ethernet

Purpose This command displays ethernet attributes.

Parameters This command has no parameters.

Command Example **Root>** show ip ethernet

Output The Ethernet attributes data is displayed as a table that includes the following properties.

IP Address	The IP address for the Ethernet adapter as set in the config.ip.ethernet command.
Gateway Address	The gateway address for the Ethernet adapter as set in the config.ip.ethernet command.
Subnet Mask	The subnet mask for the Ethernet adapter as set in the config.ip.ethernet command.

Output Example

The output from the show.ip.ethernet command displays as follows.

```

LAN Information
IP Address:      144.49.10.15
Gateway Address: 144.49.10.1
Subnet Mask:     255.255.255.0

```

show.linkIncidentLog

Syntax linkIncidentLog [clear]

Purpose This command shows the contents of the link incident log on the director or switch.

ATTENTION! If the switch is restarted (as occurs during IPL, IML, configuration reset, feature key installation, or firmware load) or is power cycled, the information in the link incident log is lost.

Parameters This command has one parameter.

clear This optional parameter causes all link incident log entries to be cleared.

Command Example **Root>** show linkIncidentLog

Output The event log data are displayed as a table that includes the following properties.

Date/Time The date and time when the event occurred.

Port The number of the port where the link incident occurred.

Link Incident Event An ASCII string describing the link incident event.

Output Example The output from the show.linkIncidentLog command displays as follows.

Date / Time	Port	Link Incident Event
02/27/03 01:28P	20	Not Operational primitive sequence (NOS) received.
02/27/03 01:28P	4	Primitive sequence timeout.
02/27/03 01:27P	62	Not Operational primitive sequence (NOS) received.
02/27/03 01:27P	62	Invalid primitive seq received for current link state

show.loginServer

Syntax loginServer

Purpose This command displays information from the login server database for devices attached to this switch. Note that it is possible to have

more than one device per port for any public loop devices attached to an FL Port.

Parameters This command has no parameters.

Command Example **Root>** show loginServer

Output The device information is displayed as a table that includes the following properties.

Port	The port number where the device is attached.
BB Crdt	The maximum number of remaining frames that can be transmitted without causing a buffer overrun condition at the receiver.
RxFldSz	The buffer-to-buffer receive data field size from the FLOGI received from the attached N_Port.
COS	The class of service (for example, 1; 2; 3; 4; 5; 6; F; 1,2; 2,3).
Port Name	The port WWN of the attached device.
Node Name	The node WWN of the attached device.

Output Example The output from the show.loginServer command displays as follows.

Port	BB Crdt	RxFldSz	COS	Port Name	Node Name
0	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
1	10		2	00:11:22:33:44:55:00:78	20:11:22:33:44:55:66:78
4	10		2,3	00:11:22:33:44:55:00:79	20:11:22:33:44:55:66:79
7	10		2,3	00:11:22:33:44:55:00:80	20:11:22:33:44:55:66:80
8	10		2	00:11:22:33:44:55:00:81	20:11:22:33:44:55:66:81
10	10		2,3	00:11:22:33:44:55:00:82	20:11:22:33:44:55:66:82
11	10		2,3	00:11:22:33:44:55:00:83	20:11:22:33:44:55:66:83
12	10		3	00:11:22:33:44:55:00:84	20:11:22:33:44:55:66:84
13	10		2,3	00:11:22:33:44:55:00:85	20:11:22:33:44:55:66:85
15	10		2,3	00:11:22:33:44:55:00:86	20:11:22:33:44:55:66:86

show.nameServer

Syntax nameServer

Purpose This command displays information from the name server database for devices attached to this switch. Note that it is possible to have more than one device per port for any public loop devices attached to an FL Port.

Parameters This command has no parameters.

Command Example **Root>** show nameServer

Output The device information data is displayed as a table that includes the following properties.

Type	The type (N, NL, F/NL, F, FL, E, B).
Port Id	The 24-bit Fibre Channel address.
Port Name	The port WWN of the attached device.
Node Name	The node WWN of the attached device.
COS	The class of service (for example, 1; 2; 3; 4; 5; 6; F; 1,2; 2,3).
FC4 Types	The FC4 types registered for this device. One or more numbers display in this field. The numbers in this field correspond to the list at the bottom of the output example below.

Output Example

The output from the show.nameServer command displays as follows.

Type	Port Id	Port Name	Node Name	COS	FC4 Types
N	010400	00:11:22:33:44:55:66:77	20:11:22:33:44:55:66:77	2,3	2
N	010500	00:11:22:33:44:55:66:78	20:11:22:33:44:55:66:78	2,3	0
N	010600	00:11:22:33:44:55:66:79	20:11:22:33:44:55:66:79	2,3	2
N	010700	00:11:22:33:44:55:66:80	20:11:22:33:44:55:66:80	2	2
N	010800	00:11:22:33:44:55:66:81	20:11:22:33:44:55:66:81	3	2
N	010900	00:11:22:33:44:55:66:82	20:11:22:33:44:55:66:82	3	2
N	010C00	00:11:22:33:44:55:66:83	20:11:22:33:44:55:66:83	2,3	2
N	010D00	00:11:22:33:44:55:66:84	20:11:22:33:44:55:66:84	2,3	2
N	010E00	00:11:22:33:44:55:66:85	20:11:22:33:44:55:66:85	2	5
N	010F00	00:11:22:33:44:55:66:86	20:11:22:33:44:55:66:86	2	4
N	011200	00:11:22:33:44:55:66:87	20:11:22:33:44:55:66:87	2,3	2
N	011300	00:11:22:33:44:55:66:88	10:11:22:33:44:55:66:88	2,3	2

FC4 Types

```

0: ISO/IEC 8802-2 LLC
1: ISO/IEC 8802-2 LLC/SNAP
2: SCSI-FCP
3: SCSI-GPP
4: IPI-3 Master
5: IPI-3 Slave
6: IPI-3 Peer
7: CP IPI-3 Master
8: CP IPI-3 Slave
9: CP IPI-3 Peer
10: SBCCS-Channel
11: SBCCS-Control Unit
12: FC-SB-2 Channel to Control Unit
13: FC-SB-2 Control Unit to Channel
14: Fibre Channel Service
15: FC-FG
16: FC-SW
17: FC-AL
18: SNMP
19: HIPPI-FP
20: Vendor Unique

```

show.nameServerExt**Syntax**

nameServerExt

Purpose

This command displays extended information from the name server database for devices attached to this switch. The command provides Symbolic Nameserver information, as well as the same information as the show.nameServer command. Multiple devices per port are possible for any public loop device attached to an FL Port.

NOTE: Because it contains symbolic nameserver information that can be lengthy, the CLI output wraps several times per node. For this reason, this command is supported only in comma-delimited mode. For more information about the comma-delimited mode, see [Using the commaDelim Command](#) on page 1-17.

Parameters This command has no parameters.

Command Example **Root>** show nameServerExt

Output The device information data is displayed as a table that includes the following properties.

Type	The type (N, NL, F/NL, F, FL, E, B).
Port Id	The 24-bit Fibre Channel address.
Port Name	The port WWN of the attached device.
Node Name	The node WWN of the attached device.
COS	The class of service (for example, 1; 2; 3; 4; 5; 6; F; 1,2; 2,3).
FC4 Types	The FC4 types registered for this device. One or more numbers display in this field. The numbers in this field correspond to the list in the output example for show.nameServer on page 2-156.
SymNodeName	255-character representation of the Symbolic Node Name.
SymPortName	255-character representation of the Symbolic Port Name.

Output Example The output from the show.nameServerExt command displays as follows.

```
Type, Port Id, Port Name, Node Name, COS, FC4 Types, SymNodeName, SymPortName,
N, 010400, 00:11:22:33:44:55:00:77, 20:11:22:33:44:55:66:77, 2-3, 2, Node Name A, Port Name A,
N, 010500, 00:11:22:33:44:55:01:77, 20:11:22:33:44:55:66:77, 2-3, 0, This Is Symbolic Node Name
B, Symbolic Port Name B Is Slightly Longer
N, 010600, 00:11:22:33:44:55:66:02, 20:11:22:33:44:55:66:77, 2-3, 2, , ,
FL, 000001, 00:11:22:33:44:55:66:03, 20:11:22:33:44:55:66:77, 2, 0, Loop Node 1, Loop Port 7
FL, 000002, 00:11:22:33:44:55:66:04, 20:11:22:33:44:55:66:77, 3, 2, Loop Node 2, Loop Port 7,
```

show.NPIV.config

Syntax config

Purpose This command displays the current NPIV configuration for all ports.

NOTE: The command [config.NPIV.show](#) on page 2-23 has functionality that is identical to this command.

Parameters This command has no parameters.

Command Example **Root>** show NPIV config

Output This command displays the following NPIV configuration data:

NPIV state The current enabled/disabled state of the NPIV feature.

Max Allowed NPIV Login Table A table mapping each port number on the switch to a corresponding max number of NPIV logins setting.

Output Example

```
NPIV state: Enabled
Port  Max Allowed NPIV Logins
----  -
1      10
2      10
3      10
4       0
5       0
7     130...
```

show.openSysMS.config

Syntax config

Purpose This command displays the Open System Management Server state and the Open System Management Server Host Control State.

Parameters This command has no parameters.

Command Example **Root>** show openSysMS config

Output The configuration data is displayed as a table that includes the following properties:

openSysMS State	The Open System Management Server state.
Host Control State	The Open System Management Server Host Control state.

Output Example

```
openSysMS State:    disable
Host Control State: enable
```

show.openTrunking.config

Syntax config

Purpose This command displays the trunking configuration for all ports.

Parameters This command has no parameters.

Command Example show openTrunking config

Output The device information data is displayed as a table that includes the following properties.

Unresolved Congestion	The current enabled/disabled state of the unresolved congestion trunking feature.
Backpressure	The current enabled/disabled state of the backpressure trunking feature.
Low BB Credit Threshold	The current threshold setting of the low BB credit threshold trunking feature listed as a percentage. If this value is configured to be the default, (default) is displayed alongside the threshold value. The default value is 75%.
Congestion Threshold Table	A table mapping each port number on the switch to a corresponding threshold setting. The threshold is listed as a percentage. If this value is configured to be the default, (default) is displayed alongside the threshold value. The default value is 60%

Output Example

The output from the show.openTrunking.config command displays as follows.

```

Unresolved Congestion:           Enabled
Backpressure:                    Disabled
Low BB Credit Threshold (%):    75 (default)
Port   Threshold %
----   -
1      60 (default)
2      69
3      60 (default)
4      60 (default)
5      90
...

```

show.openTrunking.rerouteLog

Syntax reroutelog [clear]

Purpose This command displays Open Trunking Re-route Log information.

ATTENTION! If the switch is restarted (as occurs during IPL, IML, configuration reset, feature key installation, or firmware load) or is power cycled, the information in the Open Trunking Re-route Log is lost.

Parameters This command has one parameter.

clear	This optional parameter causes all re-route log entries to be cleared.
-------	--

Command Example

```
show opentrunking reroutelog
```

NOTE: The *clear* parameter also clears the log entries for your SAN management application.

Output The device information data is displayed as a table that includes the following properties.

Date/Time	The date/time when the rerouting event occurred.
Rcv	The port associated with the flow that was rerouted.
Dom	The target domain associated with the flow that was rerouted.
Old	The exit port number on this switch that the flow used to get to the target domain.
New	The exit port number on this switch that the flow now uses to get to the target domain.

Output Example The output from the show.opentrunking.reroutelog command displays as follows.

Date/Time	RcvPort	Dom	OldExit	NewExit
-----	-----	---	-----	-----
04/12/01 10:58A	63	2	41	42
03/23/02 12:01P	4	3	35	36

show.port.config

Syntax config

Purpose This command shows the port configuration for all ports.

Parameters This command has no parameters.

Command Example **Root>** show port config

Output The port configuration attributes are displayed as a table that includes the following properties.

Port	The port number.
Name	The name of the port as set in the config.port.name command.
Blocked	The blocked state of the port as set in the config.port.blocked command.

FAN	The configured fabric address notification (FAN) state. (Sphereon 4300 and Sphereon 4500 switches only.)
Type	The port type as set in the config.port.type command.
Speed	The port speed as set in the config.port.speed command.
Rx Crdts	The number of Rx BB Credits as set in the config.port.rxCredits command.

Output Example

The output from the show.port.config command displays as follows.

Port	Name	Blocked	FAN	Type	Speed	Rx Crdts
----	-----	-----	-----	-----	-----	-----
0	Port_0_name	Blocked	Enabled	gxPort	Negotiate	12
1		Blocked	Enabled	gxPort	Negotiate	12
2		locked	Enabled	gxPort	Negotiate	12
...						

show.port.exit**Syntax**

exit destDomainID sourcePort

Purpose

This command displays the exit port from a source port to a given destination domain. This command shows the Preferred Path configuration.

Use *all* for one of the command's parameters to display all configured and actual exit ports for either the destination domain ID or the specified source Port. You cannot specify *all* for both parameters. If the destination domain is set to *all*, then all paths from the specified source port are displayed. If the source port is set to *all*, the output shows all source port paths to the specified domain.

Parameters This command has the following parameters.

destDomainId	Specifies the destination domain ID. Valid domain IDs are in the range 1–31, or, use <i>all</i> to show all exit ports to and from the source port specified in the sourcePort parameter.
sourcePort	Specifies the number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or, you can specify <i>all</i> to show all exit ports to the destination domain ID specified for the destDomainId parameter.

Output The output from show.port.exit includes the following parameters.

Destination Domain	The destination domain ID to which a preferred path has been configured. This is displayed only if the destination domain parameter is set to <i>all</i> .
Source Port	The source port for which a preferred path to the specified destination domain ID is specified. This is displayed only if the source port parameter is set to <i>all</i> .
Exit Port	This is the actual exit port being used for the given path. The value <i>No Domain</i> displays when the destination domain doesn't exist in the fabric. The value <i>No Source</i> displays when the source port is in an offline state. The value <i>Fabric Building</i> displays when the fabric is still building.

Command and Output Examples

The following examples show the output returned by the three methods of specifying the show.port.exit command.

Output with single values for both parameters

```
Root> show port exit 21 10
Exit Port: 45
```

Output with destDomainId set to all

```
Root> show port exit all 15
Destination Domain  Exit Port
-----
1                  23
2                  No Domain
3                  23
...
31                 No Domain
```

Output with sourcePort set to all

```
Root> show port exit 1 all
Source Port      Exit Port
-----
0               No Source
1               5
2               No Source
3               6
...
```

show.port.info

Syntax info

Purpose This command displays port information for all ports.

Parameters This command has no parameters.

Command Example Root> show port info

Output The port information data is displayed as a table that includes the following properties.

Port	The port number.
WWN	The WWN of the port.
OpSpeed	The current operating speed (1 Gb/sec, 2 Gb/sec, or Not Established).
SpeedCap	The current transceiver capability speed (1 Gb/sec or 2 Gb/sec).

Output Example The output from the show.port.info command displays as follows.

Port	WWN	OpSpeed	SpeedCap
0	10:00:80:00:11:22:33:44	1 Gb/sec	2 Gb/sec
1	10:00:80:01:11:22:33:44	1 Gb/sec	2 Gb/sec
2	10:00:80:02:11:22:33:44	1 Gb/sec	2 Gb/sec
3	10:00:80:03:11:22:33:44	1 Gb/sec	2 Gb/sec
4	10:00:80:04:11:22:33:44	2 Gb/sec	2 Gb/sec
5	10:00:80:05:11:22:33:44	2 Gb/sec	2 Gb/sec
6	10:00:80:06:11:22:33:44	2 Gb/sec	2 Gb/sec
7	10:00:80:07:11:22:33:44	2 Gb/sec	2 Gb/sec
8	10:00:80:08:11:22:33:44	2 Gb/sec	2 Gb/sec
9	10:00:80:09:11:22:33:44	2 Gb/sec	2 Gb/sec
10	10:00:80:10:11:22:33:44	1 Gb/sec	2 Gb/sec
11	10:00:80:11:11:22:33:44	1 Gb/sec	2 Gb/sec
12	10:00:80:12:11:22:33:44	1 Gb/sec	2 Gb/sec
13	10:00:80:13:11:22:33:44	1 Gb/sec	2 Gb/sec
14	10:00:80:14:11:22:33:44	1 Gb/sec	2 Gb/sec
15	10:00:80:15:11:22:33:44	1 Gb/sec	2 Gb/sec

show.port.nodes

Syntax nodes portNumber

Purpose This command displays the loginserver entries for a specified port. This command is valid only on the Sphereon 4300 and Sphereon 4500 switches.

Parameters This command has one parameter.

portNumber	Specifies the port number. Valid values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140
------------	---

Command Example **Root>** show port nodes portNumber

Output The port nodes data is displayed as a table that includes the following properties.

FC Addr	The Fibre Channel address of nodes attached to this port. Private devices are assigned address strings of 0000 followed by the two-digit hexadecimal Arbitrated Loop Physical Address (ALPA), instead of the 6 digit hexadecimal number presented for public devices.
BB Crdt	Represents the maximum number of outstanding frames which can be transmitted without causing a buffer over-run condition at the receiver.
RxFldSz	Buffer-to-buffer Receive Data Field Size from the FLOGI received from the attached N_Port.
COS	Class of service: 1; 2; 3; 4; 5; 6; F; 1,2; 2,3...
Port Name	The port worldwide name of the attached device.
Node Name	The node worldwide name of the attached device.

Output Example The show.port.nodes command output for a mix of public and private nodes on a loop appears as follows:

FCAddr	BB Crdt	RxFldSz	COS	Port Name	Node Name
612902	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
612903	10	2112	2	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
612904	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
612905	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
6129AB	8	2112	2	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
6129AC	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
6129AD	8		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
6129AE	10		3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
6129FD	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77
6129FE	10		2,3	00:11:22:33:44:55:00:77	20:11:22:33:44:55:66:77

show.port.opticEDD

Syntax OpticEDD

Purpose This command displays optic diagnostic information for all ports. This information is in HEX format. If there is no information available, then “Unk” will be displayed for “Unknown”.

Parameters This command has no parameters.

Command Example Show port opticEDD

Output The port optic diagnostic data is displayed as a table that includes the following properties.

Port	The port number.
Xcvr	The transceiver type.
Temp	The optic temperature in Celsius.
3.3 Voltage	The 3.3 Voltage in Volts.
Current	The Current in mA.
TX Pwr	The Transceiver power in uW.

RX Pwr The Receiver power in uW.

1.8 Voltage The 1.8 Voltage in Volts.

5.0 Voltage The 5.0 Voltage in Volts.

Output Example The show.port.opticEDD command output displays as follows:

Port	Xvr	Temp	3.3 Volt	Current	TX Power	RX Power	1.8 Volt	5.0 Volt
----	---	-----	-----	-----	-----	-----	-----	-----
0	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
1	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
2	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
3	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
4	XFP	36.105	3.256	5.324	602.100	289.300	1.779	4.998

show.port.opticInfo

Syntax OpticInfo

Purpose This command displays information about the optic.

Parameters This command has no parameters.

Command Example show port opticInfo

Output The port optic data is displayed as a table that includes the following properties.

Port The port number.

Xcvr The transceiver type.

Temp The optic temperature in Celsius.

3.3 Voltage The 3.3 Voltage in Volts.

Current The Current in mA.

TX Pwr The Transceiver power in uW.

RX Pwr The Receiver power in uW.

1.8 Voltage The 1.8 Voltage in Volts.

5.0 Voltage The 5.0 Voltage in Volts.

Output Example The show.port.opticInfo command output displays as follows:

Port	Xvr	Temp	3.3 Volt	Current	TX Power	RX Power	1.8 Volt	5.0 Volt
----	---	-----	-----	-----	-----	-----	-----	-----
0	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
1	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
2	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
3	UNK	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
4	XFP	36.105	3.256	5.324	602.100	289.300	1.779	4.998

show.port.profile

Syntax `show portNumber`

Purpose This command displays the port configuration for a single port

Parameters This command has one parameter.

portNumber Specifies the port number. Valid values are:
 0–11 for the Sphereon 4300
 0–15 for the Sphereon 3016
 0–23 for the Sphereon 4500
 0–31 for the Sphereon 3032
 0–31 for the ED-5000
 0–63 for the Intrepid 6064
 0–127 and 132–143 for the Intrepid 6140

Command Example **Root>** `show port profile portNumber 138`

Output The port profile information is displayed as a single output for an individual port.

Port Number Port number.

Name Configured port name.

Blocked Blocked state. Valid values are true and false.

Operating Type Operating port type.

Operating Speed Operating port speed.

Port WWN	Port WWN.
Configured Type	Configured port type.
Configured Speed	Configured port speed.
Beaconing	Beaconing state.
FAN	FAN state.
FC Address	The Port Fibre Channel address.
Attached WWN	The node WWN of the device at the remote end of the link. A loop port will display the first attached loop device.
Operational State	The operational state of the port.
Reason	The reason that the port operational state is not "online".
Rx BB Credits	Then number of configured Rx BB Credits.
Connector Type	Optic connector type.
Transceiver	Optic transceiver type.
Distance Capability	Optic distance capability.
Media Type	Optic media type.
Speed Capability	Optic speed capability.
10G FC Compliance	Optic 10G FC Compliance code.

Output Example

The output from the show.port.profile command displays as follows:

```

Port Number:          4
Name:                 Sam's tape drive
Blocked:              False
Operating Type:       FL Port
Operating Speed:      2 Gb/sec
Port WWN:             A2:33:15:C3:3F:00:00:0A
Configured Type:      Gx_Port
Configured Speed:     Negotiate
Beaconing:            Disabled

```



```
FAN: Disabled
FC Address: 034FA2
Attached WWN: F0:01:02:A1:B0:22:00:12
Operational State: Online
Reason: None
Rx BB Credits: 12
Connector Type: LC
Transceiver: Long LC
Distance Capability: Long
Media Type: M-M 50um
Speed Capability: 2 Gb/sec
10G FC Compliance: None
```

show.port.showPortAddr

Syntax `showPortAddr`

Purpose This command displays the port address configuration for all ports.

NOTE: The [config.port.showPortAddr](#) on page 2-28 has functionality that is identical to this command.

Parameters This command has no parameters.

Command Example `Root> show port showPortAddr`

Output The port configuration is shown as a table of properties. The following properties are displayed:

Port	The port number
Original Addr	The original port address of the port
Current Addr	The current port address of the port
Swapped Port Num	If the port is swapped with another port, it will show the port number of the port it is swapped with.

Output Example

Port	Original Addr	Current Addr	SwappedPort Num
0	4	4	
1	5	5	
2	6	7	3
3	7	6	2
4	8	8	
5	9	9	
6	a	a	
7	b	b	
8	c	c	
...			

show.port.status

Syntax status

Purpose This command displays port status for all ports.

Parameters This command has no parameters.

Command Example **Root>** show port status

Output The port status data is displayed as a table that includes the following properties.

Port	The port number.
State	The port state (for example, Segmented E_Port, Invalid Attachment, Not Installed, Online, Offline, Not Operational, No Light, Testing, Port Failure, Link Reset, or Inactive).
Type	<p>The operational port type. If the configured port type is F_Port or E_Port, this value will match the configured type. If the configured type is G_Port, this value can be E_Port, F_Port, or G_Port, depending on what is connected to the port.</p> <p>On the Sphereon 4300 and Sphereon 4500, if the configured port type is Fx_Port, the operational port type can include FL_Port in addition to the values noted above for F_Port. If the configured port type is Gx_Port, then the operational port type can include FL_Port in addition to the values noted above for G_Port.</p>

Attached WWN	The WWN of the device or switch attached to the port, if one is attached.
Beaconing	The beaconing state for the port (Off or On).
Reason	An optional message number that indicates if the port has a segmented ISL, if a port binding violation has occurred, or if the port is inactive. The message description for this message number is provided at the bottom of the table.

If the operational state is *Segmented E_Port*, only the following messages can be generated:

- 01: Segment Not Defined
- 02: Incompatible Operating Parameters
- 03: Duplicate Domain ID(s)
- 04: Incompatible Zoning Configurations
- 05: Build Fabric Protocol Error
- 06: No Principal Switch
- 07: No Response from Attached Switch
- 08: ELP Retransmission Failure Timeout

If the operational state is *Invalid Attachment* only the following messages can be generated:

- 09: Unknown
- 10: ISL connection not allowed on this port
- 11: ELP rejected by the attached switch
- 12: Incompatible switch at other end of the ISL
- 13: External loopback adapter connected to the port
- 14: N_Port connection not allowed on this port
- 15: Non-McDATA switch at other end of the ISL
- 16: ISL connection not allowed on this port
- 17: ISL connection not allowed to external Fabrics
- 18: Port binding violation - unauthorized WWN
- 19: Unresponsive Node Connected to Port
- 20: Incompatible security attributes
- 21: Fabric Binding violation
- 22: Authorization failure
- 23: Switch Binding violation

Reason (cont.)

If the operational state is *Inactive* only the following messages can be generated:

- 24: Inactive - RC 0
- 25: No Serial Number
- 26: Feature Not Enabled
- 27: Switch Speed Conflict

Output Example

The output from the show.port.status command displays as follows.

Port	State	Type	Attached WWN	Beaconing	Reason
----	-----	----	-----	-----	-----
0	Online	fPort	10:00:80:00:11:22:33:44	Off	
1	Online	gPort	10:00:80:00:11:22:33:45	On	
2	No Light	fPort	10:00:80:00:11:22:33:55	On	
3	Offline	ePort	10:00:80:00:11:22:33:00	Off	
4	Online	gPort	10:00:80:00:11:22:33:57	Off	
5	Port Failure	fPort	10:00:80:00:11:22:33:46	Off	
6	Link Reset	gPort	10:00:80:00:11:22:33:63	Off	
7	Segmented E_Port	ePort	10:00:80:00:11:22:33:47	Off	02
8	Online	ePort	10:00:80:00:11:22:33:88	Off	
9	Offline	fPort	10:00:80:00:11:22:33:49	Off	
10	Inactive	ePort	10:00:80:00:11:22:33:50	Off	26
11	Online	fPort	10:00:80:00:11:22:33:53	Off	
12	No Light	fPort	10:00:80:00:11:22:33:56	Off	
13	Online	fPort	10:00:80:00:11:22:33:59	Off	
14	Invalid Attachment	fPort	10:00:80:00:11:22:33:64	Off	15
15	Online	fPort	10:00:80:00:11:22:33:66	Off	

02: Duplicate Domain ID(s)

03: Switch Speed Conflict

07: ISL connection not allowed on this port

show.port.technology

Syntax `technology`

Purpose This command displays port technology information for all ports.

Parameters This command has no parameters.

Command Example **Root>** `show port technology`

Output The port technology data is displayed as a table that includes the following properties.

Port	The port number.
Connectr	The port connector type (LC, MT_RJ, MU, Internal).
Transcvr	The transceiver type (Long LC, Short, Short OFC, Long LL, Long Dist).
Distance	The distances supported (Short, Intermediate, Long, Very Long).
Media	The media type (M-M 62.5um, M-M 50um, M-M 50,62.5um, S-M 9um, Copper).

Output Example The output from the show.port.technology command displays as follows.

Port	Connectr	Transcvr	Distance	Media
0	LC	Long LC	Long	M-M 50um
1	LC	Long LC	Long	M-M 50um
2	LC	Long LC	Long	M-M 50um
3	MT_RJ	Long LC	Long	M-M 50um
4	MT_RJ	Long LC	Long	M-M 50um
5	MT_RJ	Long LC	Long	M-M 50um
6	LC	Long LC	Long	M-M 50um
7	LC	Long LC	Long	M-M 50um
8	LC	Long LC	Long	M-M 50um
9	LC	Long LC	Long	M-M 50um
10	LC	Long LC	Long	M-M 50um
11	LC	Long LC	Long	M-M 50um
12	LC	Long LC	Long	M-M 50um
13	LC	Long LC	Long	M-M 50um
14	LC	Long LC	Long	M-M 50um
15	LC	Long LC	Long	M-M 50um

show.preferredPath.showPath

Syntax `showPath destDomainID sourcePort`

Purpose This command displays the specified Preferred Path configuration and the actual path used by the system. The output shows both the exit port as configured for the Preferred Path feature and the actual exit port currently being used for traffic.

Use *all* for one of the command's parameters to display all configured and actual exit ports for either the destination domain ID or the specified source Port. You cannot specify *all* for both parameters. If the destination domain is set to *all*, all paths from the specified source port are displayed. If the source port is set to *all*, the output shows all source port paths to the specified domain.

Parameters This command has the following parameters.

<code>destDomainId</code>	Specifies the destination domain ID. Valid domain IDs are in the range 1–31 or <i>all</i> , which shows all paths to and from the source port specified in the <code>sourcePort</code> parameter.
<code>sourcePort</code>	Specifies the number of the source port. Valid port numbers values are: 0–11 for the Sphereon 4300 0–15 for the Sphereon 3016 and 3216 0–23 for the Sphereon 4500 0–31 for the Sphereon 3032 and 3232 0–31 for the ED-5000 0–63 for the Intrepid 6064 0–127 and 132–143 for the Intrepid 6140 Or, you can specify <i>all</i> to show all paths to the destination domain ID specified for the <code>destDomainId</code> parameter.

Output The output from `show.preferredPath.showPath` includes the following parameters.

Destination Domain	The destination domain ID to which a preferred path has been configured. This is displayed only if the destination domain parameter is set to <i>all</i> .
Source Port	The source port for which a preferred path to the specified destination domain ID is specified. This is displayed only if the source port parameter is set to <i>all</i> .
Preferred Exit Port	The configured Preferred Path exit port. This value can be any port number, or blank to indicate that no Preferred Path has been configured.
Actual Exit Port	This is the actual exit port being used for the given path.

Command and Output Examples

The following examples show the output returned by the three methods of specifying the `show.preferredPath.showPath` command.

Single values for both parameters

```
Root> show preferredPath showPath 21 10
Preferred Path State: Enabled
Preferred Exit Port:  Not Configured
Actual Exit Port:    45
```

destDomainId set to all

```
Root> show preferredPath showPath all 15
Preferred Path State: Enabled
Destination Domain  Preferred Exit Port  Actual Exit Port
-----
1                   23                   23
3                   24                   No Path
4                   23                   23
17                  12                   No Source
```

sourcePort set to all

```

Root> show preferredPath showPath 1 all
Preferred Path State: Enabled
Source Port      Preferred Exit Port  Actual Exit Port
-----
0                2                   No Source
2                5                   5
3                17                  No Path
22               5                   6
    
```

show.security.fabricBinding

Syntax fabricBinding

Purpose This command displays the fabric binding configuration saved on the fabric. The command performs the same function as config.security.fabricBinding.showActive.

Parameters This command has no parameters.

Command Example Root> show security fabricBinding

Output The fabric binding configuration data is displayed as a table that includes the following properties.

Domain ID	The domain ID of the Fabric Binding Membership List (FBML) member. Valid domain ID's range from 1 to 239.
WWN	The world wide name (WWN) of the FBML member in colon-delimited hexadecimal notation.
Attachment Status	Indicates whether the FBML member is Local, Attached, or Unattached. For more information, see Fabric Binding Membership Terminology on page 2-51.

Output Example The output from the show.security.fabricBinding command displays as follows.

```

Domain 1 (20:30:40:50:60:70:8F:1A) (Local)
Domain 3 (00:11:22:33:44:55:66:77) (Unattached)
Domain 2 (88:99:AA:BB:CC:DD:EE:FF) (Attached)
Domain 14 (11:55:35:45:24:78:98:FA) (Attached)
    
```

show.security.log

Syntax log [clear]

Purpose This command shows the contents of the security log as maintained in NV-RAM on the director or switch.

Parameters This command has one parameter.

clear This optional parameter causes all security log entries to be cleared.

Command Example **Root>** show security log

Output The security log data are displayed as a table that includes the following properties.

Reason	The reason code for the security event.
Date/Time	The date and time when the event occurred.
Trigger Level	The trigger level of the event. Possible values may be: Informational, Security Change, or Error.
Category	The event category message. Possible values may be: Successful Connection, Disconnection, Configuration Change, Authorization Failure, Authentication Failure, or Reserved.
Count	A cumulative count of events within a known period.
Desc	A formatted string containing a description of the event.
Data	A formatted string containing additional or event-specific data.

Output Example The output from the show.security.log command displays as follows.

Reason	Date/Time	Trigger Level	Category	Count
10000	04/12/01 10:58A	Informational	Successful Connection	375
Desc: EWS User Connected				

```
Data: Usr=Administrator IPAddr=001.002.003.004 Role=admin
10305 04/11/01 01:03A Error Authorization Failure 1
Desc: IP Access Control List Violation
Data: IPAddr=172.072.016.097 SrcPort=0072 DestPort=0124
10300 04/02/01 08:30P Error Authorization Failure 3
Desc: Fabric Binding Mismatch
Data: Prt=0100 NbrW=02:15:F4:2A:11:0F:11:00 NbrDID=004 ErrDID=001
10411 03/31/01 02:24A Error Authentication Failure 1
Desc: OS Management Server Authentication Not Provided
Data: Port=0100 WWN=01:02:03:04:05:06:07:08
```

show.security.portBinding

Syntax portBinding

Purpose This command shows the port binding configuration for all ports.

Parameters This command has no parameters.

Command Example **Root>** show security portBinding

Output The port binding configuration data is displayed as a table that includes the following properties.

Port	The port number.
WWN Binding	The state of port binding for the specified port (active or inactive).
Bound WWN	The WWN of the device that is bound to the specified port. If this field is blank, no device is bound to the specified port.

Output Example The output from the show.security.portBinding command displays as follows.

Port	WWN Binding	Bound WWN
----	-----	-----
0	Active	AA:00:AA:00:AA:00:AA:00
1	Inactive	00:00:00:00:00:00:00:00
2	Inactive	CC:33:44:55:CC:33:44:55
3	Active	00:00:00:00:00:00:00:00
4	Inactive	00:00:00:00:00:00:00:00
5	Inactive	00:00:00:00:00:00:00:00
6	Inactive	00:00:00:00:00:00:00:00
7	Inactive	00:00:00:00:00:00:00:00
8	Inactive	00:00:00:00:00:00:00:00
9	Inactive	00:00:00:00:00:00:00:00
10	Inactive	00:00:00:00:00:00:00:00
11	Inactive	00:00:00:00:00:00:00:00
12	Inactive	00:00:00:00:00:00:00:00
13	Inactive	00:00:00:00:00:00:00:00
14	Inactive	00:00:00:00:00:00:00:00
15	Inactive	00:00:00:00:00:00:00:00

show.security.switchAcl

Syntax switchAcl

Purpose This command displays the contents of the Switch Access Control List.

Parameters This command has no parameters.

Command Example **Root>** show security switchACL

Output The data is displayed as a table that includes the following properties:

Switch ACL State	The enabled state of the Switch Access Control List
Starting IP Address	The starting IP Address of a range in the access control list.
Ending IP Address	The ending IP Address of a range in the access control list.

Output Example

ACL State: Disabled	
Starting IP Address	Ending IP Address
-----	-----
110.80.1.1	110.80.255.255
110.81.1.10	110.81.1.255
200.11.15.1	200.11.255.128

show.security.switchBinding

Syntax switchBinding

Purpose This command displays the switch binding configuration.

Parameters This command has no parameters.

Command Example **Root>** show security switchBinding

Output The switch binding configuration data is displayed as a table that includes the following properties.

Switch Binding State	The switch binding state, which can have the following values:
----------------------	--

Disabled

Enabled and Restricting F_Ports

Enabled and Restricting E_Ports

Enabled and Restricting All Ports

Switch Binding Membership List	The WWNs of the members of the active SBML.
--------------------------------	---

Output Example The output from the show.security.switchBinding command displays as follows.

```
Switch Binding State:   Enabled and Restricting E Ports
00:11:22:33:44:55:66:77
88:99:AA:BB:CC:DD:EE:FF
11:55:35:45:24:78:98:FA
```

show.snmp

Syntax `snmp`

Purpose This command shows the switch SNMP configuration.

Parameters This command has no parameters.

NOTE: The command [config.snmp.show](#) on page 2-71 has functionality that is identical to this command.

Command Example **Root>** `show snmp`

Output The switch configuration data is displayed as a table that includes the following properties.

SNMP Agent State	The state of the SNMP agent. If it is disabled, the SNMP state does not respond to any requests and does not produce any traps.
FA MIB Version Number	Version of the MIB that the SNMP agent is configured to use.
Authentication Traps	The state of the authentication traps (for example, enabled) that are sent to SNMP management stations when unauthorized stations attempt to access SNMP information from the switch.
Index	The community index number.
Community Name	The name of the community.
WriteAuth	The write authorization state.
Trap Recipient	The address of the trap recipient shown in 4-byte dotted-decimal format.
UDP Port	The user datagram protocol (UDP) port number to which the director or switch will send traps for each recipient.

Output Example

The output from the show.snmp command displays as follows.

```
SNMP Agent State:      Enabled
FA MIB Version Number: 3.0
Authentication Traps:  Enabled
Index  Community Name      WriteAuth  Trap Recipient  UDP Port
-----
1      CommunityName1      Enabled    123.123.123.123  162
2      CommunityName2      Enabled    10.25.25.10      144
3      CommunityName3      Disabled   132.44.85.224    162
4      public                Enabled    132.44.85.224    162
5
```

show.switch

Syntax switch

Purpose This command displays switch attributes.

Parameters This command has no parameters.

Command Example **Root>** show switch

Output The switch attributes data is displayed as a table that includes the following properties.

State	The state of the switch (for example, online or offline).
BB Credit	The BB_Credit. (This does not apply to the Sphereon 4300 and Sphereon 4500 switches.)
R_A_TOV	The R_A_TOV as set in the config.switch.raTOV command. For more information, see config.switch.raTOV on page 2-76.
E_D_TOV	The E_D_TOV as set in the config.switch.edTOV command. For more information, see config.switch.edTOV on page 2-73.
Preferred Domain Id	The domain ID as set in the config.switch.prefDomainId command. For more information, see config.switch.prefDomainId on page 2-75.

Switch Priority	The switch priority as set in the <code>config.switch.priority</code> command. For more information, see config.switch.priority on page 2-75.
Speed	The switch speed as set in the <code>config.switch.speed</code> command. (This does not apply to the Sphereon 4300 and Sphereon 4500 switches.) For more information, see config.switch.speed on page 2-78.
Rerouting Delay	The rerouting delay as set in the <code>config.switch.rerouteDelay</code> command. For more information, see config.switch.rerouteDelay on page 2-77.
Interop Mode	The interoperability mode as set in the <code>config.switch.interopMode</code> command. For more information, see config.switch.interopMode on page 2-74.
Active Domain Id	The active domain ID of the switch. This ID may or may not be the same as the preferred domain ID.
World Wide Name	The WWN for the switch.
Insistent Domain Id	Configured Insistent domain ID state as set in the <code>config.switch.insistDomainId</code> command. For more information, see config.switch.insistDomainId on page 2-73.
Domain RSCN	Configured Domain RSCN state as set in the <code>config.switch.domainRSCN</code> command. For more information, see config.switch.domainRSCN on page 2-72.
Zoning RSCN	Configured Zoning RSCN state as set in the <code>config.switch.zoningRSCN</code> command. For more information, see config.switch.zoningRSCN on page 2-81.
FC Address Domain Id	The domain ID of the switch derived from the Fibre Channel Address.
Limited Fabric RSCN	When enabled, fabric RSCNs are suppressed after an IPL.

Output Example

The output from the show.switch command displays as follows.

```

State:                               Online
BB Credit:                           2
R_A_TOV:                             20
E_D_TOV:                             4
Preferred Domain Id:                 1
Switch Priority:                     Default
Speed:                              2 Gb/sec
Rerouting Delay:                     Enabled
Interop Mode:                       Open Fabric 1.0
Active Domain Id:                    1
World Wide Name:                    10:00:08:00:88:00:21:07
Insistent Domain Id:                 Enabled
Domain RSCN:                         Enabled
Zoning RSCN:                         Disabled
FC Address Domain Id:                67 (hexadecimal)
Limited Fabric RSCN:                 Disabled

```

show.system**Syntax**

system

Purpose

This command displays a set of system attributes.

Parameters

This command has no parameters.

Command Example

Root> show system

Output

The system attributes are displayed as a table that includes the following properties.

Name	The system name as set in the config.system.name command. For more information, see config.system.name on page 2-83.
Contact	The system contact as set in the config.system.contact command. For more information, see config.system.contact on page 2-81.
Description	The system description as set in the config.system.description command. For more information, see config.system.description on page 2-82.

Location	The system description as set in the <code>config.system.description</code> command. For more information, see config.system.location on page 2-83.
Serial Number	The serial number for the system.
Type Number	The type number for the system.
Model Name	The model name for the system (for example, Sphereon 4500).
Model Number	The model number for the system. All products have the model number <i>001</i> , except 1 Gb sheet metal units, which are <i>002</i> .
EC Level	The engineering change level installed.
Firmware Version	The current firmware version installed.
Beaconing	The enabled state of unit beaconing (enabled or disabled) as set in the <code>maint.system.beacon</code> command.
Date/Time	The system date and time as set in the <code>config.system.date</code> command. For more information, see config.system.date on page 2-82.

Output Example The output from the `show.system` command displays as follows.

```
System Information
Name:                Joe's Switch
Description:         McDATA ED-6064 Fibre Channel Director
Contact:             Joe
Location:            Everywhere
Date/Time:           04/16/2001  10:34:01AM
Serial Number:       82420481
Type Number:         006064
Model Name:          ED-6064
Model Number:        001
EC Level:            1011231
Firmware Version:    04.01.00 Build 23
Beaconing:           Disabled
```

show.thresholdAlerts.alerts

Syntax alerts

Purpose This command provides the name, type, and enabled state of each configured threshold alert, including both counter threshold alerts (CTAs) and throughput threshold alerts (TTAs).

Parameters This command has no parameters.

Command Example **Root>** show thresholdAlerts alerts

Output The threshold alert data displays as a table that includes the following properties.

Name	The name of the threshold alert, truncated to 45 characters.	
Type	The trigger statistic or threshold type of the alert (abbreviated to 17 characters). These include:	
	Tx Util	TTA - Transmit Utilization
	Rx Util	TTA - Receive Utilization
	Tx/Rx Util	TTA - Transmit or Receive Utilization
	Link Resets Sent	CTA - Link Resets Sent
	Link Resets Received	CTA - Link Resets Received
	OLS Sent	CTA - OLS Sent
	OLS Received	CTA - OLS Received
	Link Failures	CTA - Link Failures
	Sync Losses	CTA - Sync Losses
	Signal Losses	CTA - Signal Losses
	Protocol Errors	CTA - Primitive Sequence Errors/Protocol Errors
	Invalid Tx Words	CTA - Invalid Tx Words
	CRC Errors	CTA - CRC Errors
	Discarded Frames	CTA - Discarded Frames
	Frames Too Short	CTA - Frames Too Short

Delimiter Errors	CTA - Delimiter Errors
Address ID Errors	CTA - Address ID Errors
Cls2 BusiedFrms	CTA - Class 2 Busied Frames
Cls2 RejectedFrms	CTA - Class 2 Rejected Frames
Cls3 DiscardFrms	CTA - Class 3 Discarded Frames
Phys Lnk Err Set	CTA - Physical Link Errors Summed Set
Lnk Seq Cnt Set	CTA - Link Sequence Counts Summed Set
Logic Lnk Err Set	CTA - Logical Link Errors Summed Set
LIPS Detected	CTA - Loop Initialization Primitives Detected (Sphereon 4300 and 4500 only)
LIPS Generated	CTA - Loop Initialization Primitives Generated (Sphereon 4300 and 4500 only)
State	The enabled state of the CTA, either <i>enabled</i> or <i>disabled</i> .

Output Example The output from the show.thresholdAlerts.alerts command displays as follows.

Name	Type	State
Throughput Threshold #1	Rx Util	Enable
Threshold for CRC	CRC Errors	Disabled
Safety #2	Logic Lnk Err Set	Enabled
Safety #1	Cls2 BusiedFrms	Disabled

show.thresholdAlerts.log

Syntax log [clear]

Purpose This command shows the contents of the threshold alert log. This log shows all the threshold alerts that have been triggered, including both counter threshold alerts (CTAs) and throughput threshold alerts (TTAs).

ATTENTION! If the switch is restarted (as occurs during IPL, IML, configuration reset, feature key installation, or firmware load) or is power cycled, the information in the threshold alert log is lost.

Parameters This command has one parameter.

clear	This optional parameter causes all threshold log entries to be cleared.
-------	---

Command Example **Root>** show thresholdAlerts log

Output The threshold alert log data displays as a table that includes the following properties.

Date/Time	The date and time of the alert.
Name	The name of the threshold alert, truncated to 22 characters.
Port	The type of threshold alert (CTAs only).
Type	The trigger statistic or threshold type of the alert (abbreviated to 17 characters). These include:
Tx Util	TTA - Transmit Utilization
Rx Util	TTA - Receive Utilization
Tx/Rx Util	TTA - Transmit or Receive Utilization
Link Resets Sent	CTA - Link Resets Sent
Link Resets Received	CTA - Link Resets Received
OLS Sent	CTA - OLS Sent

OLS Received	CTA - OLS Received
Link Failures	CTA - Link Failures
Sync Losses	CTA - Sync Losses
Signal Losses	CTA - Signal Losses
Protocol Errors	CTA - Primitive Sequence Errors/Protocol Errors
Invalid Tx Words	CTA - Invalid Tx Words
CRC Errors	CTA - CRC Errors
Discarded Frames	CTA - Discarded Frames
Frames Too Short	CTA - Frames Too Short
Delimiter Errors	CTA - Delimiter Errors
Address ID Errors	CTA - Address ID Errors
Cls2 BusiedFrms	CTA - Class 2 Busied Frames
Cls2 RejectedFrms	CTA - Class 2 Rejected Frames
Cls3 DiscardFrms	CTA - Class 3 Discarded Frames
Phys Lnk Err Set	CTA - Physical Link Errors Summed Set
Lnk Seq Cnt Set	CTA - Link Sequence Counts Set
Logic Lnk Err Set	CTA - Logical Link Error Set
LIPS Detected	CTA - Loop Initialization Primitives Detected (Sphereon 4300 and 4500 only)
LIPS Generated	CTA - Loop Initialization Primitives Generated (Sphereon 4300 and 4500 only)

Value The increment or utilization value of the alert.

Interval The time interval of the alert.

Output Example The output from the show.thresholdAlerts.log command displays as follows:

Date/Time	Name	Port	Type	Value	Int
05/26/02 10:58A	CTA Alert #4	2	Cls3 DiscardFrms	250	10
05/24/02 12:01A	CTA Alert #4	2	Cls3 DiscardFrms	250	10
05/22/02 10:58A	My test CTA	43	CRC Errors	35	30
05/20/02 08:01P	TTA Test #3	2	Tx Util	85	120
03/01/02 02:58A	CTA Alert #1	130	CRC Errors	100	60

show.zoning

Syntax zoning

Purpose This command shows the zoning configuration saved on the fabric.

Parameters This command has no parameters.

Command Example **Root>** show zoning

Output The zoning configuration data is displayed as a table that includes the following properties.

Active ZoneSet The enabled status, name, and member zones of the zone set.

Output Example The output from the show.zoning command displays as follows.

```
Active Zone Set
Default Zone Enabled: False
ZoneSet: TheUltimateZoneSet
  Zone: TheUltimateZone
    ZoneMember: Domain 10, Port 6
    ZoneMember: Domain 15, Port 2
    ZoneMember: Domain 2, Port 63
    ZoneMember: 10:00:00:00:C9:22:9B:64
    ZoneMember: 10:00:00:00:C9:22:9B:BD
  Zone: TheNotSoUltimateZone
    ZoneMember: 10:00:00:00:C9:22:9B:AB
    ZoneMember: 10:00:00:00:C9:22:9B:C6
    ZoneMember: 10:00:00:00:C9:22:9B:AB
  Zone: TheNotUltimateAtAllZone
    ZoneMember: Domain 2, Port 63
```


This appendix lists and explains error messages for the Command Line Interface (CLI). Any error numbers that are not listed are reserved for future use.

The message that is returned is a string that includes the error number and the text of the message.

Message	Error 005: Busy
Description	The switch cannot process any requests at this time.
Action	Re-submit the request.
Message	Error 007: Not Authorized
Description	You are unable to get write authorization to save the configuration
Action	Try again later.
Message	Error 008: Invalid Switch Name
Description	The value entered for the switch name is invalid.
Action	The name for the director or switch may contain 0–24 characters. Enter a name with 0–24 characters and re-submit. If spaces are used, enclose the name in quotation marks.

Message	Error 009: Invalid Switch Description
Description	The value entered for the switch DESCRIPTION is invalid.
Action	The description for the director or switch may contain 0–255 characters. Enter a description with 0–255 characters and re-submit. If spaces are used, enclose the description in quotation marks.
Message	Error 010: Invalid Switch Location
Description	The value entered for the switch location is invalid.
Action	The location for the director or switch may contain 0–255 characters. Enter a location with 0–255 characters and re-submit. If spaces are used, enclose the location in quotation marks.
Message	Error 011: Invalid Switch Contact
Description	The value entered for the switch contact is invalid.
Action	The contact for the director or switch may contain 0–255 characters. Enter a contact with 0–255 characters and re-submit. If spaces are used, enclose the contact in quotation marks.
Message	Error 012: Invalid Port Address
Description	The value entered for the port address is invalid.
Action	Enter a valid port address.
Message	Error 013: Invalid Port Number
Description	The value entered for the port number is invalid.
Action	Enter a port number within the range supported by your director or switch.

Message	Error 014: Invalid Port Name
Description	The value entered for the port name is invalid.
Action	The port name for the individual port may contain 0–24 characters. Enter a name with 0–24 characters and re-submit. If spaces are used, enclose the name in quotation marks.
Message	Error 015: Invalid BB Credit
Description	The value entered for the buffer-to-buffer credit is invalid.
Action	The buffer-to-buffer credit must be an integer in the range of 1–60.
Message	Error 016: Invalid R_A_TOV
Description	The value entered for the resource allocation time-out value is invalid.
Action	The R_A_TOV is entered in tenths of a second and must be entered as an integer in the range 10–1200 (1 second to 120 seconds). The R_A_TOV value must be larger than the E_D_TOV value. Check to be sure that all conditions are met and re-submit.
Message	Error 017: Invalid E_D_TOV
Description	The value entered for the error detection time-out value is invalid.
Action	The E_D_TOV is entered in tenths of a second and must be entered as an integer in the range 2–600 (0.2 second to 60 seconds). The E_D_TOV must be smaller than the R_A_TOV. Check to be sure that all conditions are met and re-submit.
Message	Error 018: Invalid TOV
Description	The E_D_TOV and R_A_TOV values are not compatible.
Action	Enter a valid E_D_TOV / R_A_TOV combination. The E_D_TOV must be smaller than the R_A_TOV.

Message	Error 020: Invalid Preferred Domain ID
Description	The value entered for the preferred domain ID for the director or switch is invalid.
Action	The preferred domain ID must be an integer in the range 1–31. Enter an appropriate value and re-submit.
Message	Error 021: Invalid Switch Priority
Description	The value entered for the switch priority is invalid.
Action	The switch priority entered for the director or switch must be one of the following: principal, neverprincipal, or default. Enter an appropriate value and re-submit. (Refer to the description of the command in config.switch.priority on page 2-75.)
Message	Error 029: Invalid Gateway Address
Description	The value entered for the gateway address is invalid.
Action	The new gateway address for the Ethernet interface must be entered in dotted decimal format (e.g. 0.0.0.0). Enter an appropriate gateway address and re-submit.
Message	Error 030: Invalid IP Address
Description	The value entered for the IP Address is invalid.
Action	The new IP address for the Ethernet interface must be entered in dotted decimal format (e.g. 10.0.0.0). Enter an appropriate IP address and re-submit.
Message	Error 031: Invalid Subnet Mask
Description	The value entered for the subnet mask is invalid.
Action	The new subnet mask for the Ethernet interface must be entered in dotted decimal format (e.g. 255.0.0.0). Enter an appropriate subnet mask and re-submit.

Message	Error 032: Invalid SNMP Community Name
Description	The value entered for the SNMP community name is invalid
Action	The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and re-submit.
Message	Error 033: Invalid SNMP Trap Address
Description	The value entered for the SNMP trap address is invalid.
Action	The new SNMP trap address for the SNMP interface must be entered in dotted decimal format (e.g. 10.0.0.0). Enter an appropriate SNMP trap address and re-submit.
Message	Error 034: Duplicate Community Names Require Identical Write Authorization
Description	Two or more community names have been recognized as being identical, but their corresponding write authorizations are not identical.
Action	Enter unique SNMP community names or force write authorizations for duplicate community names to be identical and re-submit.
Message	Error 036: Port Already Swapped
Description	The port has already been swapped with another port and cannot be swapped again.
Action	Unswap the port before swapping it with another port

Message	Error 037: Invalid Month
Description	The value of the month entered for the new system date is invalid.
Action	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The month must contain an integer in the range 1–12. Enter an appropriate date and re-submit.
Message	Error 038: Invalid Day
Description	The value of the day entered for the new system date is invalid.
Action	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The day must contain an integer in the range 1–31. Enter an appropriate date and re-submit.
Message	Error 039: Invalid Year
Description	The value of the year entered for the new system date is invalid.
Action	The format of the date parameter must be mm:dd:yyyy or mm/dd/yyyy. The year must contain an integer greater than 1980. Enter an appropriate date and re-submit.
Message	Error 040: Invalid Hour
Description	The value of the hour entered for the new system time is invalid.
Action	The format of the time parameter must be hh:mm:ss. The hour can contain an integer in the range 0–23. Enter an appropriate time and re-submit.
Message	Error 041: Invalid Minute
Description	The value of the minute entered for the new system time is invalid.
Action	The format of the time parameter must be hh:mm:ss. The minute can contain an integer in the range 0–59. Enter an appropriate time and re-submit.

Message	Error 042: Invalid Second
Description	The value of the second entered for the new system time is invalid.
Action	The format of the time parameter must be hh:mm:ss. The second can contain an integer in the range 0–59. Enter an appropriate time and re-submit.
Message	Error 044: Max SNMP Communities Defined
Description	A new SNMP community may not be defined without removing an existing community from the list.
Action	A total of 6 communities may be defined for SNMP. A new community can be added only after a current community is removed. Make the appropriate changes and re-submit.
Message	Error 045: Not Allowed While Switch Online
Description	The entered command requires that the director or switch be set offline.
Action	Set the switch offline and re-submit the command.
Message	Error 047: LIC install Active
Description	Cannot perform the specified action while a firmware download is in progress.
Action	Wait until the firmware download is complete and try again.
Message	Error 049: Invalid RADIUS Server UDP Port Number
Description	The RADIUS server UDP port number entered is invalid.
Action	Enter a valid UDP port. Valid values are 1 to 65535

Message	Error 050: Invalid RADIUS Server Timeout Value
Description	The RADIUS server Timeout value entered is invalid.
Action	Enter a valid Timeout value. Valid values are 1 to 1000.
Message	Error 051: Invalid RADIUS Server Transmit Attempts Value
Description	The RADIUS server Retransmit value entered is invalid.
Action	Enter a valid Retransmit value. Valid values are 1 to 100.
Message	Error 052: Invalid RADIUS Server Deadtime Value
Description	The RADIUS server Deadtime entered is invalid.
Action	Enter a valid Deadtime value. Valid values are 0 to 1440.
Message	Error 053: Invalid RADIUS Key
Description	The RADIUS key entered is invalid.
Action	Enter a valid RADIUS key. Key length must be no more than 256 characters.
Message	Error 054: Buffer Limit Exceeded
Description	The total number of BB Credits configured cannot exceed the BB Credit buffer pool limit.
Action	Configure the total number of BB Credits for this switch to be less than or equal to the buffer pool limit.
Message	Error 055: Invalid Zone Name
Description	The value entered for the zone name is invalid.
Action	The zone name must be unique and contain 1–64 characters. The valid character set for the zone name can be found under

[config.zoning.renameZoneSet](#) on page 2-91. Make the appropriate changes to the zone name and re-submit.

Message **Error 057: Duplicate Zone**

Description Two or more zone names in the zone set are identical.

Action All zone names must be unique. Make the appropriate changes and re-submit.

Message **Error 059: Zone Name in Use**

Description Two or more zone names in the zone set are identical.

Action All zone names must be unique. Make the appropriate changes and re-submit.

Message **Error 060: Invalid Number of Zone Members**

Description The entered command tried to add more zone members than the zone can hold.

Action Reduce the number of zone members in the zone and re-submit the command.

Message **Error 061: Invalid Zone Member Type**

Description A zone member was entered that is neither a WWN nor a Domain, Port pair.

Action Zone members must be expressed in WWN format or as a Domain, Port pair. Make the appropriate changes and re-submit. For more information, see [config.zoning.clearZone](#) on page 2-88 and [config.zoning.addPortMem](#) on page 2-86.

Message	Error 062: Invalid Zone Set Name
Description	The value entered for the zone set name is invalid.
Action	The zone set name must be contain 1–64 characters. The valid character set for the zone name can be found in config.zoning.renameZoneSet on page 2-91. Make the appropriate changes to the zone set name and re-submit.
Message	Error 064: Configuration changes have been limited to the API interface
Description	The API interface has restricted this interface from making configuration changes.
Action	To make configuration changes from this interface, the API interface will need to update to allow this interface to make changes.
Message	Error 065: Cannot remove the last CLI user with Administrator rights
Description	There has to be at least one CLI user with Administrator rights.
Action	To remove this user, add another CLI Administrator and then delete this user.
Message	Error 068: The Switch IP Access Control List is Full
Description	The list being activated has an invalid number of IP pairs
Action	Make sure there is at least one IP address in the Access Control List
Message	Error 069: Duplicate Port Name
Description	Two or more port names are identical.
Action	Port names must be unique. Make appropriate changes and re-submit. For more information, see config.port.name on page 2-26.

Message	Error 070: Invalid FRU Type
Description	The requested FRU does not exist on this product.
Action	Consult the installation/service manual for this product to find appropriate FRU names.
Message	Error 071: FRU Not Installed
Description	The requested FRU is not installed.
Action	Consult the installation/service manual for this product for appropriate action.
Message	Error 072: No Backup FRU
Description	The FRU swap cannot be performed because a backup FRU is not installed.
Action	Insert a backup FRU and re-submit the request or consult the installation/service manual for this product for appropriate action.
Message	Error 073: Port Not Installed
Description	The port specified is not installed on this product.
Action	Consult the installation/service manual on installing a port optic.
Message	Error 074: Invalid Number of Zones
Description	The specified zone set contains less than one zone or more than the maximum number of zones allowed for this product.
Action	A zone set must contain at least one zone to be considered valid. Add or remove zones accordingly to meet specified requirements.

Message	Error 075: Invalid Zone Set Size
Description	The zone set entered exceeds switch NVRAM limitations.
Action	Reduce the size of the zone set to meet specified requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.
Message	Error 076: Invalid Number of Unique Zone Members
Description	The zone entered contains more than the maximum number of zone members allowed per zone set for this product.
Action	Reduce the number of members in one or more zones and re-submit the command.
Message	Error 077: Not Allowed While Port Is Failed
Description	The port selected is in a failed or inactive state, or is in need of service.
Action	Consult the installation/service manual for appropriate action.
Message	Error 078: System Error Light On
Description	This unit is not able to beacon because the system error light is on.
Action	You must clear the system error light before unit beaconing may be enabled. Consult the installation/service manual for appropriate action.
Message	Error 079: FRU Failed
Description	The specified FRU has failed.
Action	Consult the installation/service manual for appropriate action.

Message	Error 081: Default Zone Enabled
Description	The request cannot be completed because the default zone is enabled
Action	Disable the default zone and re-submit the command.
Message	Error 082: Invalid Interop Mode
Description	The value entered for the interoperability mode is not valid.
Action	The interoperability mode for the director or switch must be mcdata (McDATA Fabric 1.0) or open (Open Fabric 1.0). Make the appropriate changes and re-submit the command.
Message	Error 083: Not Allowed in Open Fabric Mode
Description	This request cannot be completed while this switch is operating in Open Fabric 1.0 mode.
Action	Configure the interop mode to McDATA Fabric 1.0 mode.
Message	Error 088: Invalid Feature Key Length
Description	The feature key installed is longer than the maximum length allowed.
Action	Be sure that the key has been entered correctly and re-submit. Contact your sales representative with any further problems.
Message	Error 090: Invalid Port Type
Description	The port type configured is invalid.
Action	A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and re-submit the command.

Message	Error 091: E_Port Type Configured
Description	Ports are not allowed to be configured as E_Ports in S/390 mode.
Action	Configure the port as either a fport or gport and resubmit the command.
Message	Error 092: Not Allowed While Port Is Unblocked
Description	The port must be blocked to complete this request.
Action	Block the port and re-submit the command.
Message	Error 093: Not Allowed While FICON MS Is Installed
Description	This request cannot be completed because FICON Management Server is installed.
Action	This operation is not supported. No action necessary.
Message	Error 094: Invalid Feature Combination
Description	The features requested cannot be installed at the same time on one switch or director.
Action	Contact your sales representative.
Message	Error 099: Preferred Domain ID Cannot Be Zero
Description	This product cannot be configured to have a preferred domain ID equal to zero (0).
Action	Ensure that the ID is expressed as an integer in the range 1–31 and re-submit.

Message	Error 101: Command Not Supported on This Product
Description	This product does not support the requested command.
Action	Command not supported. No action necessary.
Message	Error 102: Switch Not Operational
Description	The request cannot be completed because the switch is not operational.
Action	Consult the installation/service manual and contact your service representative.
Message	Error 103: Port Diagnostic In Progress
Description	The request cannot be completed because a port diagnostic is running.
Action	Wait for the diagnostic to complete.
Message	Error 104: System Diagnostic In Progress
Description	The request cannot be completed because a system diagnostic is running.
Action	Wait for the diagnostic to complete.
Message	Error 105: Max Threshold Definitions Reached
Description	The maximum number of total threshold alerts has already been reached.
Action	Remove a threshold alert before adding the new threshold alert. A total of 16 counter and throughput threshold alerts is allowed.

Message	Error 106: Invalid Threshold Scope
Description	The scope of a threshold alert is not set to a valid state before the user activates an alert.
Action	Set the scope of the threshold alert, then try to activate the alert.
Message	Error 107: Invalid Threshold State
Description	The scope of a threshold alert must be set before the user activates an alert.
Action	Set the scope of the threshold alert, then try to activate the alert.
Message	Error 108: Invalid TTA Type
Description	The type of the throughput threshold alert has not been set.
Action	Set the type of the TTA, then try to activate the alert.
Message	Error 109: Invalid CTA Type
Description	The type of the counter threshold alert has not been set.
Action	Set the type of the CTA, then try to activate the alert.
Message	Error 110: Invalid Percent Utilization
Description	The type of the throughput threshold alert has not been set.
Action	Set the type of the TTA, then try to activate the alert.
Message	Error 111: Invalid Threshold Type
Description	The type of the threshold alert is not valid.
Action	Configure the type of the throughput threshold alert to one of the types found in the enumerated table for TTAs.

Message	Error 112: No Threshold Definition Given
Description	The threshold value for the alert was not configured before the user attempted to activate the alert.
Action	Set the threshold value, then try to activate the alert.
Message	Error 115: Invalid Switch Speed
Description	The request cannot be completed because the switch is not capable of operating at the configured speed.
Action	Consult the installation/service manual to determine the speed capabilities of your product.
Message	Error 116: Switch Not Capable of 2 Gb/sec
Description	The request cannot be completed because the switch is not capable of operating at 2 Gb/sec.
Action	Consult the installation/service manual to determine the speed capabilities of your product.
Message	Error 117: Port Speeds Cannot be Set at Higher Data Rate than Switch Speed
Description	This request cannot be completed because the requested port speed is faster than the currently-configured switch speed.
Action	The switch speed should first be configured to accommodate changes in the configured port speed. The ports cannot operate at a faster rate than the switch, itself. Update the switch speed and re-submit the request. For more information, see config.switch.speed on page 2-78 and config.port.show on page 2-27.

Message	Error 118: Invalid Port Speed
Description	This request cannot be completed because the requested port speed is not recognized for this product.
Action	Port speeds may be set to 1 Gb/s or 2 Gb/s. Update the port speed and re-submit the request.
Message	Error 119: Switch Speed Not 2 Gb/sec
Description	This request cannot be completed because the switch speed has not been set to 2 Gb/s.
Action	The switch speed must be set to 2 Gb/s in order to accommodate a port speed of 2 Gb/s. Update the switch speed and re-submit the request.
Message	Error 121: Invalid Credit Starvation Threshold
Description	An invalid credit starvation threshold has been entered.
Action	Submit the request with a valid value. The credit starvation threshold must be in the range 1-99.
Message	Error 122: Invalid Port Congestion Threshold
Description	An invalid port congestion threshold has been entered.
Action	Submit the request with a valid value. The port congestion threshold must be in the range 1-99.
Message	Error 134: Invalid Membership List
Description	Generic message to indicate a problem in either the switch binding or fabric binding membership list.
Action	Be sure that the membership list submitted does not isolate a switch already in the fabric. If this is not the case, the user needs to be aware of all fabric security rules and make sure that the list submitted adheres appropriately.

Message	Error 135: Invalid Number of Fabric Membership List Entries
Description	The number of fabric members submitted exceeds the maximum allowable entries of 31.
Action	The number of entries in the fabric membership list is limited to the total number of domain IDs available to the fabric. Make sure that the list (including the managed switch) contains no more than 31 entries.
Message	Error 136: Invalid Number of Switch Binding Membership List Entries
Description	The number of switch members submitted exceeds the maximum allowable entries of 256.
Action	The number of entries in the Switch Binding Membership List is limited to 256. Make sure that the list (including the managed switch) contains no more than 256 entries.
Message	Error 137: Invalid Fabric Binding State
Description	The fabric binding state submitted is not recognized by the CLI.
Action	The fabric binding state must be set to either “inactive” or “restrict.” See config.security.fabricBinding on page 2-51 for clarification on these states.
Message	Error 138: Invalid Switch Binding State
Description	The switch binding state submitted is not recognized by the CLI.
Action	The switch binding state must be set to one of the following: <i>disable</i> , <i>erestrict</i> , <i>frestrict</i> , or <i>allrestrict</i> . See config.security.switchBinding on page 2-64 for clarification on these states.

Message	Error 139: Insistent Domain ID's Must Be Enabled When Fabric Binding Active
Description	The user attempted to disable insistent domain IDs while fabric binding was active.
Action	Insistent domain IDs must remain enabled while fabric binding is active. If fabric binding is set to inactive, the insistent domain ID state may be changed. It should be noted, however, that this can be disruptive to the fabric.
Message	Error 140: Invalid Insistent Domain ID State
Description	The request cannot be completed because an invalid insistent domain ID state has been submitted.
Action	The insistent domain ID state must be set to either <i>enable</i> or <i>disable</i> . For more information, see config.switch.insistDomainId on page 2-73.
Message	Error 141: Invalid Enterprise Fabric Mode
Description	The request cannot be completed because an invalid enterprise fabric mode has been submitted.
Action	The enterprise fabric mode must be set to either <i>activate</i> or <i>deactivate</i> . For more information, see config.enterpriseFabMode.setState on page 2-5.
Message	Error 142: Invalid Domain RSCN State
Description	The request cannot be completed because an invalid domain RSCN state has been submitted.
Action	The domain RSCN state must be set to either <i>enable</i> or <i>disable</i> . For more information, see config.switch.domainRSCN on page 2-72.

Message	Error 143: Domain RSCNs Must Be Enabled When Enterprise Fabric Mode Active
Description	The user attempted to disable domain RSCN's while enterprise fabric mode was active.
Action	Domain RSCN's must remain enabled while the enterprise fabric mode is active. If enterprise fabric mode is set to inactive, the domain RSCN state may be changed. It should be noted, however, that this can be disruptive to the fabric.
Message	Error 144: The SANtegrity Feature Has Not Been Installed
Description	The user attempted to activate a change to the fabric security configuration without first installing the SANtegrity feature key.
Action	If this key has not been installed, contact your sales representative.
Message	Error 146: Fabric Binding May Not Be Deactivated While Enterprise Fabric Mode Active
Description	The user attempted to deactivate fabric binding while enterprise fabric mode was active.
Action	Fabric binding must be active while operating in enterprise fabric mode. The fabric binding state may be changed if enterprise fabric mode is deactivated. It should be noted, however, that this can be disruptive to the fabric.
Message	Error 147: Cannot Complete Request While SW Trunking Is Enabled
Description	Cannot perform this action because the SW Trunking feature is enabled.
Action	Disable the SW Trunking feature.

Message	Error 148: Not Allowed While Switch Offline
Description	The switch must be online to complete this request.
Action	Change the state of the switch to ONLINE and re-submit the request.
Message	Error 149: Not Allowed While Enterprise Fabric Mode Enabled and Switch Active
Description	The request cannot be completed while the switch is online and enterprise fabric mode is Active.
Action	This operation will be valid if the switch state is set to offline and enterprise fabric mode to inactive. It should be noted, however, that this can be disruptive to the fabric.
Message	Error 151: Invalid Open Systems Management Server State
Description	The request cannot be completed because the OSMS state submitted is invalid.
Action	The OSMS state may be set to either <i>enable</i> or <i>disable</i> . For more information, see config.features.openSysMS on page 2-8.
Message	Error 152: Invalid FICON Management Server State
Description	The request cannot be completed because the FICON MS state submitted is invalid.
Action	The FICON MS state may be set to either <i>enable</i> or <i>disable</i> . For more information, see config.ficonMS.setMIHPTO on page 2-19.
Message	Error 153: Feature Key Not Installed
Description	The request cannot be completed because the required feature key has not been installed to the firmware.
Action	Contact your sales representative.

Message	Error 154: Invalid Membership List WWN
Description	The request cannot be completed because the WWN does not exist in the switch binding membership list.
Action	Make sure that the WWN deleted matches the WWN in the Switch Binding Membership List. Make appropriate changes and re-submit the request.
Message	Error 155: Cannot Remove Active Member From List
Description	This member cannot be removed from the fabric security list because it is currently logged in.
Action	Fabric security rules prohibit any device or switch from being isolated from the fabric via a membership list change. If it is truly the intention of the user to remove the device in question from the membership list, then there are several approaches to take. This request may be completed most non-disruptively by blocking the port (or physically removing the device from the managed switch) to which this device is attached and resubmitting the request.
Message	Error 156: Cannot Complete While Switch is Online and Fabric Binding Active
Description	The switch must be offline and Fabric Binding must be inactive before this feature can be disabled.
Action	Deactivating this feature can be disruptive to Fabric operations. Take the switch offline and make sure deactivate fabric binding before disabling this feature.
Message	Error 157: Access Control List is Disabled
Description	The switch must be offline and Fabric Binding must be inactive before this feature can be disabled.
Action	Deactivating this feature can be disruptive to Fabric operations. Take the switch offline and deactivate fabric binding before disabling this feature.

Message	Error 158: Invalid Switch IP Access Control List IP Address Range
Description	The pair of IP addresses are invalid and cannot be added to the list.
Action	Make sure the IP addresses are valid and the first IP is lower than the second.
Message	Error 159: Invalid IP Access Control List Pairs Count Value
Description	The list being activated has an invalid number of IP pairs.
Action	Make sure there is at least one IP address in the Access Control List.
Message	Error 161: The Switch IP Access Control List is Empty
Description	The management interface IP address is not in the list.
Action	The management IP must be in the list or the current connection would be lost.
Message	Error 162: List is full
Description	There is no more room for new entries in the list.
Action	Remove a different entry and try again.
Message	Error 163: FICON MS feature key must be installed
Description	The command is not available without the FICON MS feature key.
Action	Install the FICON MS feature key.
Message	Error 164: FICON CUP Zoning feature key must be uninstalled
Description	The operation cannot be completed with the FICON CUP Zoning key installed.
Action	Remove the FICON CUP Zoning feature key.

Message	Error 165: CUP Zoning feature key must be installed
Description	The command is not available without the FICON CUP Zoning feature key.
Action	Install the FICON CUP zoning feature key.
Message	Error 166: CUP Zoning feature must be enabled
Description	The command cannot be completed with the CUP Zoning feature enabled.
Action	Enable FICON CUP Zoning.
Message	Error 167: Diagnostics can not be run on inactive port
Description	The port is in the inactive state and diagnostics cannot be run.
Action	The port state must change out of the inactive state.
Message	Error 168: Duplicate member in the list
Description	The member is already in the list.
Action	Duplicate members are not allowed in the list.
Message	Error 169: Cannot enable CNT feature
Description	CNT support is in the wrong state.
Action	The enabled state for CNT support must be changed.
Message	Error 170: Duplicate IP Address range in the switch IP Access Control List
Description	Duplicate IP address pairs are not allowed in the Access Control List.
Action	This command is redundant, the member already exists in the list.

Message	Error 171: Invalid username
Description	The username is invalid.
Action	Enter a unique username using only the allowed characters and proper length.
Message	Error 172: Invalid list size
Description	The number of entries in the list is invalid.
Action	Make sure the list has at least one entry.
Message	Error 173: Invalid value
Description	The value being entered is invalid.
Action	Enter a valid value.
Message	Error 174: Invalid list data
Description	The list data is invalid.
Action	Correct the list to make it a valid list.
Message	Error 175: Invalid list index (the user should not see this error)
Description	The index in the list is incorrect.
Action	Correct the index.
Message	Error 176: Entry not found in the list
Description	The desired entry in the list does not exist.
Action	Make sure the desired entry is in the list and it is being typed correctly.

Message	Error 177: Cannot remove the last Web user with Administrator rights
Description	At least one Administrator user must exist for each management interface.
Action	Add a new Administrator and then try again.
Message	Error 178: Invalid password
Description	The entered password is invalid.
Action	Enter a password using valid characters and a proper length.
Message	Error 179: Insistent Domain IDs must be enabled
Description	To complete this command, Insistent Domain IDs must be enabled.
Action	Enabled Insistent Domain IDs.
Message	Error 180: Too many management interface users
Description	Only 25 management users can be added to the user database.
Action	Remove other management users in order to make room for a new one.
Message	Error 181: Preferred path must be disabled
Description	The Preferred Path feature must be disabled.
Action	Disable the Preferred Path feature.
Message	Error 182: Invalid fencing policy state
Description	The current fencing state is invalid.
Action	Enter a valid fencing state.

Message	Error 183: Invalid Enable Status
Description	The enable status is invalid.
Action	Enter a valid enable status.
Message	Error 184: Invalid Fencing Policy Time Period
Description	The entered period is invalid.
Action	Enter a valid period.
Message	Error 185: Invalid Limit Value for this Fencing Policy Type
Description	The entered limit is invalid.
Action	Enter a valid limit.
Message	Error 186: Cannot Block this Port
Description	Port is not blockable.
Action	Enter a valid port number.
Message	Error 187: Cannot Beacon this Port
Description	Cannot enable beaconing on this port.
Action	Enter a valid port number.
Message	Error 188: Port Swap Classification is not Identical
Description	Cannot swap ports because the port swap classification is not identical.
Action	Swap different ports or install a FRU with the same port classification.

Message	Error 189: Invalid Fencing Policy Type
Description	Invalid fencing policy type.
Action	Enter a valid fencing policy type.
Message	Error 190: Invalid Fencing Policy Port Type
Description	Invalid fencing policy port type.
Action	Enter a valid port or port type.
Message	Error 191: Max Fencing Policy Definitions Reached
Description	A new port fencing policy may not be defined without removing an existing port fencing policy from the list.
Action	A total of 14 policies may be defined for port fencing. A new policy can be added only after a current policy is removed. Make the appropriate changes and re-submit.
Message	Error 192: Invalid Fencing Policy Name
Description	Port fencing name is invalid.
Action	Configure a valid port fencing name.
Message	Error 193: Cannot Modify an Enabled Fencing Policy
Description	The policy is cannot be modified while it is enabled.
Action	Disabled the policy before modifying.

Message	Error 194: Cannot enable two policies of the same type that contain the same ports
Description	Two policies of the same type cannot be enabled if they have ports that are in both lists.
Action	Make sure the policy that is being enabled doesn't have the same port number as a policy that is enabled
Message	Error 195: Cannot enable two policies of the same type that contain same port scope
Description	Two policies of the same type cannot be enabled if they have the same port type.
Action	Make sure the policy that is being enabled doesn't have the same port type as a policy that is enabled.
Message	Error 196: Cannot enable two policies of the same type that contain default scope
Description	Two policies of the same type cannot be enabled if they are both using the default ports.
Action	Enable only one policy that is using the default ports.
Message	Error 197: Port list contains no ports
Description	The policy port list must contain ports or a port scope.
Action	Add ports or a port scope to the policy.
Message	Error 198: Duplicate Authentication Name
Description	Authentication names must be unique.
Action	Configure a unique authentication name.

Message	Error 201: Change Authorization Request Failed
Description	The switch did not accept the request to make a change to NVRAM.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Message	Error 202: Invalid Change Authorization ID
Description	The switch will not accept a change request from this particular client.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Message	Error 203: Another Client Has Change Authorization
Description	Another user is currently making changes to this switch.
Action	Be sure all parameters have been entered correctly and re-submit.
Message	Error 207: Change Request Failed
Description	The switch did not accept the request.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Message	Error 208: Change Request Timed Out
Description	Authorization time to make NVRAM changes has expired.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.

Message	Error 209: Change Request Aborted
Description	The switch did not accept the request.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with further problems.
Message	Error 210: Busy Processing Another Request
Description	A different switch in the Fabric was busy processing another request and could not complete the command.
Action	Be sure all parameters have been entered correctly and re-submit. Contact your service representative with continued problems.
Message	Error 211: Duplicate Zone
Description	Two or more zone names in the local zone set are identical.
Action	All zone names must be unique. Make the appropriate changes and re-submit.
Message	Error 212: Duplicate Zone Member
Description	A member was added that already exists in the zone.
Action	No action necessary.
Message	Error 213: Number of Zones Is Zero
Description	You are attempting to activate an empty zone set.
Action	The zone set must have at least one zone to be considered valid. Add a valid zone to the zone set and re-submit.

Message	Error 214: A Zone Contains Zero Members
Description	You are attempting to activate a zone set that contains at least one zone with zero members.
Action	Each zone in the zone set must contain at least one member. Add a valid member to the empty zone and re-submit.
Message	Error 215: Zone Set Size Exceeded
Description	The local work area zone set has outgrown the size limitations imposed by the Command Line Interface.
Action	Reduce the size of the zone set to meet CLI requirements. This can be a reduction in the number of zones in the zone set, a reduction of members in a zone, or a reduction of zone name lengths.
Message	Error 216: No Attached Nodes Exist
Description	There are no attached nodes.
Action	To add more members, attach more devices to the switch or add the members by WWN or Domain ID and port.
Message	Error 217: All Attached Nodes are in the Zone
Description	All the attached nodes are already in the zone.
Action	To add more members, attach more devices to the switch or add the members by WWN or Domain ID and port.
Message	Error 218: Invalid Port Number
Description	The value entered for the port number is invalid
Action	Enter a port number within the range supported by your director or switch.

Message	Error 219: Invalid Port Type
Description	The port type configured is invalid.
Action	A port may be configured to be an eport, gport, or fport. Be sure the port is configured appropriately and re-submit the command. On the Sphereon 4300 and Sphereon 4500 only, fxport and gxport types are also supported. On the Sphereon 4300, the Fabric Capable feature must be installed to configure a E_Port, G_Port, or Gx_Port.
Message	Error 220: Cannot run diagnostics while a device is logged in to the port
Description	Diagnostics cannot be run while a device is logged into the port.
Action	Block the port to run diagnostics.
Message	Error 221: Cannot run diagnostics on an active E Port
Description	Diagnostics cannot be run on an active E Port.
Action	Block the port to run diagnostics.
Message	Error 222: Invalid SNMP Community Index
Description	The value entered for the SNMP community index is invalid.
Action	The SNMP community index must be an integer in the range 1–6. Make the appropriate changes and re-submit the command.
Message	Error 223: Unknown Error
Description	The switch did not accept the request.
Action	Contact your service representative.

Message	Error 224: Invalid Argument
Description	One or more parameters are invalid for this command.
Action	Consult this manual (Chapter 2, CLI Commands) for appropriate parameter names. Parameters must be typed exactly to specification to be recognized correctly by the CLI.
Message	Error 226: Argument Is Too Long
Description	One or more parameters are invalid for this command.
Action	For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.
Message	Error 227: Invalid SNMP Community Name
Description	The value entered for the SNMP community name is invalid.
Action	The community name must not exceed 32 characters in length. Duplicate community names are allowed, but corresponding write authorizations must match. Enter an appropriate SNMP community name and re-submit.
Message	Error 228: Invalid Write Authorization Argument
Description	The writeAuthorization parameter does not contain a valid value.
Action	Parameters must be typed exactly to specification to be recognized correctly by the CLI. For more information, see config.snmp.addCommunity on page 2-68.
Message	Error 229: Invalid UDP Port Number
Description	The udpPortNum parameter does not contain a valid value.
Action	Parameters must be typed exactly to specification to be recognized correctly by the CLI. For more information, see config.switch.insistDomainId on page 2-73.

Message	Error 230: Invalid WWN
Description	The wwn parameter does not contain a valid value.
Action	For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.
Message	Error 231: Invalid Port number
Description	The portNum parameter does not contain a valid value.
Action	For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.
Message	Error 232: Invalid Domain ID
Description	The domainID parameter does not contain a valid value.
Action	For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.
Message	Error 233: Invalid Member
Description	The zone member added is not valid.
Action	For the appropriate parameters, see the section of the manual that corresponds to the attempted command. Parameters must be typed exactly to specification to be recognized correctly by the CLI.

Message Error 234: Invalid Command

Description The CLI cannot associate an action with the submitted command. The command may be misspelled, required parameters may be missing, or the request may not be applicable to the branch of the CLI tree from which it was submitted.

Action Consult the documentation for the command to be sure this command was entered correctly, all parameters are valid and present, and that the syntax is correct.

Message Error 235: Unrecognized Command

Description The CLI does not recognize the command and cannot perform the help '?' command as requested.

Action The entered command is misspelled or the prompt is not positioned at the right place in the CLI command tree for this command. For the appropriate syntax, see the section of the manual that corresponds to the attempted command.

Message Error 236: Ambiguous Command

Description The CLI does not recognize the command issued.

Action The CLI cannot interpret the command because a unique match cannot be identified. For the appropriate syntax, see the section of the manual that corresponds to the attempted command. Enter the complete command and re-submit.

Message Error 237: Invalid Zoning Database

Description There was an unidentifiable problem in the local zone set work area.

Action Verify all parameters are entered correctly and re-submit. Otherwise, the pending zone set should be cleared and reconstructed.

Message	Error 238: Invalid Feature Key
Description	The feature key entered is invalid.
Action	Verify that the feature key was entered correctly and re-submit. Contact your service representative with further difficulties.
Message	Error 239: Fabric binding entry not found
Description	The user requested to remove a fabric binding entry that is not in the pending fabric membership list.
Action	Verify that the correct entry (both WWN and Domain ID) is being requested for removal from the list and re-submit the request.
Message	Error 240: Duplicate fabric binding member
Description	The user requested to add an entry to the fabric binding list that is already a member of the list.
Action	Verify that the correct entry (both WWN and Domain ID) is being requested for addition to the list and re-submit the request.
Message	Error 241: Comma-delimited mode must be active
Description	Comma-delimited mode must be active to execute this command
Action	Some commands require that comma-delimited mode be active (e.g. show.nameserverExt). Enable comma-delimited mode and re-issue the command.
Message	Error 244: Not allowed when Enterprise Fabric Mode is Active and Switch is Online
Description	This operation is not allowed while the switch is in Enterprise Fabric Mode and the switch is Online.
Action	Make sure Enterprise Fabric Mode is not enabled and the switch is offline.

Message	Error 245: Invalid increment value
Description	The increment value specified is not between 1 and 70560.
Action	Make sure the increment value given is between 1 and 70560.
Message	Error 246: Invalid interval value
Description	The interval value specified is not between 5 and 70560 minutes.
Action	Make sure the increment value given is between 5 and 70560 minutes.
Message	Error 247: Invalid counter number
Description	The counter specified is not a valid number.
Action	Use the table output by the command <code>perf.counterThreshAlerts.showStatisticsTable</code> to find a valid counter value.
Message	Error 248: A counter must be assigned to this threshold alert
Description	A counter must be assigned to an alert before it is enabled.
Action	Use the <code>perf.counterThreshAlerts.setCounter</code> command to set a counter before the alert is enabled.
Message	Error 249: At least one port or port type must be added to this threshold alert
Description	A port or port type must be assigned to an alert before it is enabled.
Action	Use the <code>perf.counterThreshAlerts.addPort</code> command to add a port before the alert is enabled.

Message	Error 250: Invalid counter threshold alert name
Description	The name specified for the alert is not valid.
Action	Specify a counter threshold alert name that has already been created.
Message	Error 251: The threshold alert must be disabled
Description	The counter threshold alert to be modified/deleted is already enabled.
Action	Disable the threshold alert and then try the command again.
Message	Error 253: Cannot Remove a Member Currently Interacting with the Fabric
Description	Current members of the fabric must be included in the Fabric Binding List.
Action	Do not remove active fabric members from the pending Fabric Binding Membership List.
Message	Error 254: A utilization type must be assigned to this threshold alert
Description	A utilization type must be set before activating this threshold alert.
Action	Add a utilization type and then the threshold alert can be activated.
Message	Error 255: Invalid throughput threshold alert name
Description	The name of the threshold alert is incorrect.
Action	Either the name does not exist, or the new name cannot be used because it is illegal or a duplicate.

Message	Error 256: Invalid utilization type number
Description	The utilization type number does not exist.
Action	Select a valid utilization type number.
Message	Error 257: Invalid utilization percentage value
Description	The utilization percentage value is out of range.
Action	Select a valid utilization percentage value.
Message	Error 258: Invalid duration value
Description	The duration value in minutes is out of range.
Action	Select a valid duration value.
Message	Error 259: Invalid threshold alert name
Description	The name of the threshold alert is incorrect.
Action	The threshold alert name does not exist.
Message	Error 260: Not Allowed when SANtegrity feature is not installed on remote switch
Description	All switches in the fabric must have the SANtegrity feature key installed.
Action	Install the SANtegrity feature key on all switches in the fabric.
Message	Error 261: No Attached Members Exist
Description	There are no members attached to the switch.
Action	Check all connections and make sure attached devices are present.

Message	Error 262: All Attached Members are in the Membership List
Description	All attached fabric members are already in the membership list.
Action	This action is redundant, all members are already in the list.
Message	Error 263: The SANtegrity Authentication feature key is not installed
Description	The SANtegrity Authentication feature key is not installed.
Action	Install the SANtegrity Authentication feature key.
Message	Error 264: The Preferred Path feature key is not installed
Description	The preferred path feature key must be installed.
Action	Install the preferred path feature key.
Message	Error 265: Duplicate threshold alert name
Description	The desired name for the threshold alert is already in use.
Action	Use a different name for the threshold alert.
Message	Error 266: Attached members cannot be added while fabric is building
Description	Attached members cannot be added while the fabric is building.
Action	The fabric is still building, wait a couple of seconds until it is complete.
Message	Error 268: RADIUS key too long
Description	The desired RADIUS key is too long.
Action	Use a shorter RADIUS key.

Message	Error 269: Invalid retransmit attempts. Must be between 1 and 100
Description	The desired retransmit attempt value is invalid.
Action	Select a retransmit value between 1 and 100.
Message	Error 270: Invalid timeout value. Must be between 1 and 1000
Description	The desired retransmit value is invalid.
Action	Select a timeout value between 1 and 10000.
Message	Error 271: Invalid deadtime value. Must be between 0 and 1440 minutes
Description	The desired deadtime value is invalid.
Action	Select a deadtime value between 0 and 1440.
Message	Error 272: Invalid IP address and port combination
Description	The desired host name and port combination doesn't exist in the database or it is invalid.
Action	Select a valid host name and port combination.
Message	Error 273: Passwords do not match
Description	The password does not match the confirm password.
Action	Re-enter the command and enter matching passwords.
Message	Error 274: Invalid interface combination
Description	The desired interface is not a valid interface.
Action	Select a valid interface value.

Message	Error 275: Invalid authentication role
Description	The desired role is not a valid role.
Action	Select a valid role. Valid roles are administrator and operator.
Message	Error 276: Invalid sequence authentication combination
Description	The desired sequence is not a valid sequence.
Action	Select a valid sequence. Valid sequences are RADIUS, local, and RADIUS local.
Message	Error 277: Roles cannot be assigned to a username with this interface
Description	The role of the selected username is not configurable.
Action	This operation is not supported. No action necessary.
Message	Error 278: CHAP authenticated passwords must be exactly 16 bytes
Description	The CHAP authentication password must be exactly 16 bytes.
Action	Enter a CHAP authentication password that is exactly 16 bytes.
Message	Error 280: Zone Member doesn't exist
Description	The desired zone member doesn't exist.
Action	Select a valid zone member.
Message	Error 281: Zone doesn't exist
Description	The desired zone doesn't exist.
Action	Select a valid zone name.

Message	Error 282: Conflicting Domain ID for the specified WWN
Description	The desired Domain ID is already in use.
Action	Select a different Domain ID.
Message	Error 283: Conflicting WWN for the specified Domain ID
Description	The WWN is already in use.
Action	Select a different WWN.
Message	Error 284: FICON CUP Zoning host control list is full
Description	A new host may not be entered without removing an existing host from the list.
Action	A total of 8 hosts may be defined for the FICON CUP Zoning host control list. A new host can be added only after a current host is removed. Make the appropriate changes and re-submit.
Message	Error 285: WWN not found in host control list
Description	The desired WWN is not in the host control list.
Action	Select a WWN that is in the host control list.
Message	Error 286: Invalid number of NPIV allowed logins
Description	The desired value for NPIV allowed logins is invalid.
Action	Select a value between 1 and 256.
Message	Error 287: Port is unaddressable
Description	The desired port cannot be configured because it is unaddressable.
Action	This operation is not supported. No action necessary.

Message	Error 288: The NPIV feature key must be installed
Description	The NPIV feature key must be installed to complete this operation.
Action	Install the NPIV feature key.
Message	Error 289: Duplicate policy name
Description	A policy cannot be added if it has the same name as an existing policy.
Action	Select a different policy name.
Message	Error 290: No Optic Installed
Description	There is not an optic in the port for the specified port number.
Action	Select a different port number, or plug in an optic.
Message	Error 291: Port Inaccessible
Description	There port in inaccessible for the given port number.
Action	Select a different port number.
Message	Error 292: Port Number out of Range
Description	The specified port number if out of range for the given switch/director.
Action	Select a different port number.
Message	Error 294: Invalid RADIUS Index
Description	The specified RADIUS index is invalid.
Action	Enter a valid RADIUS index. Valid indexes are 1 to 3.

Message	Error 295: Invalid MIHPTO value
Description	The MIHPTO value is invalid.
Action	Enter a valid MIHPTO value.
Message	Error 296: Cannot delete last EPort user with current authentication setting
Description	You cannot remove the last EPort user with the current authentication settings.
Action	Modify the EPort authentication settings.
Message	Error 297: Cannot delete last NPort user with current setting authentication setting
Description	You cannot remove the last NPort user with the current authentication settings.
Action	Modify the Nport authentication settings.
Message	Error 298: Cannot delete last API user with current authentication setting
Description	You cannot remove the last API user with the current authentication settings.
Action	Modify the API authentication settings.

Message	Error 299: Chap secret not defined
Description	The Chap secret must be defined (for Open Systems Management Server before enabling Outgoing Authentication.)
Action	Define a Chap Secret (for Open Systems Management Server).
Message	Error 300: No user defined for this Interface
Description	You cannot perform the specified action unless a user is defined for the interface.
Action	Create a user for the interface.
Message	Error 301: RADIUS server undefined
Description	You cannot perform the operation until a RADIUS server is configured. (You cannot enable RADIUS Authentication if there is not RADIUS server configured.)
Action	Configure a RADIUS server (before enabling RADIUS Authentication).
Message	Error 302: Pending Default Zone Member Count Exceeds Threshold
Description	You cannot enable default zoning if there are more than 64 devices not being zoned.
Action	Bring the number of unzoned devices down to 64.
Message	Error 303: Invalid Preferred Path
Description	The preferred path entered is invalid. (One reason the preferred path could be invalid is if the destination domain ID is the same as the local switch's.)
Action	Enter a valid preferred path.

Message	Error 304: Radius Authentication Present. Cannot remove all Radius Servers
Description	You cannot remove all the RADIUS Server configurations if RADIUS Authentication is enabled on any interface.
Action	Disabled RADIUS Authentication on all interfaces and then remove the last RADIUS server configuration.
Message	Error 305: Operating mode is not OSMS
Description	You cannot enable CT Outgoing Authentication when Open Systems Management Server is disabled.
Action	Enabled Open Systems Management Server before enabling CT Outgoing Authentication.
Message	Error 306: CT Outgoing Authentication is enabled
Description	You cannot disable Open Systems Management Server when CT Outgoing Authentication is enabled.
Action	Disabled CT Outgoing Authentication before disabling Open Systems Management Server.
Message	Error 307: The preferred path does not exist
Description	You tried to clear a path that does not exist.
Action	None
Message	Error 308: Invalid line speed combination
Description	The ethernet speed/duplex combination is invalid.
Action	Enter a valid ethernet speed/duplex combination.

Commands and Corresponding Releases

Table B-1, *Commands and Releases*, shows the commands that are valid in the Enterprise Operating System (E/OS) Command Line Interface (CLI) and the release in which the command was added to the CLI. The commands are organized by release, and are in alphabetical order within the release.

Table B-1 **Commands and Releases**

First E/OS Release	Command
7.0	config.features.NPIV
7.0	config.fencing.addPolicy
7.0	config.fencing.addPort
7.0	config.fencing.deletePolicy
7.0	config.fencing.removePort
7.0	config.fencing.setParams
7.0	config.fencing.setState
7.0	config.fencing.show
7.0	config.fencing.showTypeTable
7.0	config.ficonCUPZoning.addControlHost
7.0	config.ficonCUPZoning.deleteControlHost
7.0	config.ficonCUPZoning.setState

Table B-1 Commands and Releases

First E/OS Release	Command
7.0	config.ficonCUPZoning.show
7.0	config.ficonMS.setMIHPTO
7.0	config.ficonMS.show
7.0	config.ip.lineSpeed
7.0	config.NPiv.maxPortIDs
7.0	config.NPiv.setState
7.0	config.NPiv.show
7.0	config.openSysMS.setHostCtrlState
7.0	config.port.rxCredits
7.0	config.port.show
7.0	config.port.showPortAddr
7.0	config.port.swapPortByAddr
7.0	config.port.swapPortByNum
7.0	config.security.authentication.interface.api.outgoing
7.0	config.security.authentication.interface.api.sequence
7.0	config.security.authentication.interface.cli.sequence
7.0	config.security.authentication.interface.eport.outgoing
7.0	config.security.authentication.interface.eport.sequence
7.0	config.security.authentication.interface.nport.outgoing
7.0	config.security.authentication.interface.nport.sequence
7.0	config.security.authentication.interface.osms.outgoing
7.0	config.security.authentication.interface.osms.setKey
7.0	config.security.authentication.interface.serial.enhancedAuth
7.0	config.security.authentication.interface.show
7.0	config.security.authentication.interface.web.sequence

Table B-1 Commands and Releases

First E/OS Release	Command
7.0	config.security.authentication.port.override
7.0	config.security.authentication.port.show
7.0	config.security.authentication.RADIUS.attempts
7.0	config.security.authentication.RADIUS.deadtime
7.0	config.security.authentication.RADIUS.deleteServer
7.0	config.security.authentication.RADIUS.server
7.0	config.security.authentication.RADIUS.show
7.0	config.security.authentication.RADIUS.timeout
7.0	config.security.authentication.switch.setSecret
7.0	config.security.authentication.user
7.0	config.security.authentication.user.add
7.0	config.security.authentication.user.delete
7.0	config.security.authentication.user.modify
7.0	config.security.authentication.user.role
7.0	config.security.authentication.user.show
7.0	config.security.ssh.resetKeys
7.0	config.security.ssh.setState
7.0	config.security.ssh.show
7.0	config.security.switchAcl.addRange
7.0	config.security.switchAcl.deleteRange
7.0	config.security.switchAcl.deleteRange
7.0	config.security.switchAcl.setState
7.0	config.security.switchAcl.show
7.0	config.switch.zoneFlexPars
7.0	perf.preferredPath.showPath

Table B-1 Commands and Releases

First E/OS Release	Command
7.0	perf.thresholdAlerts.show
7.0	show.auditLog
7.0	show.epFrameLog.config
7.0	show.epFrameLog.filterClassFFrames
7.0	show.epFrameLog.noWrap
7.0	show.epFrameLog.setFilterPort
7.0	show.epFrameLog.wrap
7.0	show.fabricLog.noWrap
7.0	show.fabricLog.wrap
7.0	show.fabric.principal
7.0	show.fencing.policies
7.0	show.ficonCUPZoning
7.0	show.ficonMS
7.0	show.NPIV.config
7.0	show.openSysMS.config
7.0	show.port.config
7.0	show.port.opticsEDD
7.0	show.port.opticsInfo
7.0	show.port.profile
7.0	show.port.showPortAddr
7.0	show.security.switchAcl
7.0	show.security.log
7.0	show.security.switchAcl
6.1	config.snmp.setFaMibVersion
6.1	config.snmp.setState

Table B-1 Commands and Releases

First E/OS Release	Command
6.1	perf.preferredPath.clearPath
6.1	perf.preferredPath.setPath
6.1	perf.preferredPath.setState
6.1	perf.preferredPath.showPath
6.1	show.all
6.1	show.fabric.nodes
6.1	show.fabric.topology
6.1	show.linkIncidentLog
6.1	show.port.exit
6.1	show.preferredPath.showPath
6.1	show.thresholdAlerts.alerts
6.1	show.thresholdAlerts.log
5.3	config.enterpriseFabMode.setState
5.3	config.features.openTrunking
5.3	config.ficonMS.setMIHPTO
5.3	config.NPIV.maxPortIDs
5.3	config.switch.ltdFabRSCN
5.3	config.switch.zoningRSCN
5.3	perf.openTrunking.backPressure
5.3	perf.openTrunking.congestionThresh
5.3	perf.openTrunking.lowBBCreditThresh
5.3	perf.openTrunking.setState
5.3	perf.openTrunking.show
5.3	perf.openTrunking.unresCongestion
5.3	perf.thresholdAlerts

Table B-1 Commands and Releases

First E/OS Release	Command
5.3	show.openTrunking.config
5.3	show.openTrunking.rerouteLog
4.0	config.features.enterpriseFabMode
4.0	config.features.ficonMS
4.0	config.features.installKey
4.0	config.features.openSysMS
4.0	config.features.show
4.0	config.ip.ethernet
4.0	config.ip.show
4.0	config.port.blocked
4.0	config.port.fan
4.0	config.port.name
4.0	config.port.show
4.0	config.port.speed
4.0	config.port.type
4.0	config.security.fabricBinding
4.0	config.security.portBinding
4.0	config.security.switchBinding
4.0	config.snmp.addCommunity
4.0	config.snmp.addCommunity
4.0	config.snmp.authTraps
4.0	config.snmp.deleteCommunity
4.0	config.snmp.show
4.0	config.switch
4.0	config.switch.domainRSCN

Table B-1 Commands and Releases

First E/OS Release	Command
4.0	config.switch.edTOV
4.0	config.switch.insistDomainId
4.0	config.switch.interopMode
4.0	config.switch.prefDomainId
4.0	config.switch.priority
4.0	config.switch.raTOV
4.0	config.switch.rerouteDelay
4.0	config.switch.show
4.0	config.switch.speed
4.0	config.system.contact
4.0	config.system.date
4.0	config.system.description
4.0	config.system.location
4.0	config.system.name
4.0	config.system.show
4.0	config.zoning.activateZoneSet
4.0	config.zoning.addPortMem
4.0	config.zoning.clearZone
4.0	config.zoning.renameZoneSet
4.0	config.zoning.clearZone
4.0	config.zoning.renameZoneSet
4.0	config.zoning.deactivateZoneSet
4.0	config.zoning.deletePortMem
4.0	config.zoning.renameZone
4.0	config.zoning.renameZoneSet

Table B-1 Commands and Releases

First E/OS Release	Command
4.0	config.zoning.renameZone
4.0	config.zoning.renameZoneSet
4.0	config.zoning.replaceZoneSet
4.0	config.zoning.setDefZoneState
4.0	config.zoning.showActive
4.0	config.zoning.showPending
4.0	maint.port.beacon
4.0	maint.port.reset
4.0	maint.system.beacon
4.0	maint.system.clearSysError
4.0	maint.system.ipl
4.0	maint.system.resetConfig
4.0	maint.system.setOnlineState
4.0	perf.class2
4.0	perf.class3
4.0	perf.clearStats
4.0	perf.errors
4.0	perf.link
4.0	perf.traffic
4.0	show.eventLog
4.0	show.features
4.0	show.frus
4.0	show.ip.ethernet
4.0	show.loginServer
4.0	show.nameServer

Table B-1 Commands and Releases

First E/OS Release	Command
4.0	show.nameServerExt
4.0	show.port.config
4.0	show.port.info
4.0	show.port.nodes
4.0	show.port.status
4.0	show.port.technology
4.0	show.security.fabricBinding
4.0	show.security.portBinding
4.0	show.security.switchBinding
4.0	show.switch
4.0	show.system
4.0	show.zoning

This glossary includes terms and definitions from:

- *American National Standard Dictionary for Information Systems* (ANSI X3.172-1990), copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 25 West 42nd Street, New York, NY 10036. Definitions from this text are identified by (A).
- *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronic Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions from this text are identified by (E).
- *IBM Dictionary of Computing* (ZC20-1699). Definitions from this text are identified by (D).
- *Information Technology Vocabulary*, developed by Subcommittee 1 (SC1), Joint Technical Committee 1 (JTC1), of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Definitions of published parts of this vocabulary are identified by (I). Definitions taken from draft international standards, committee drafts, and working papers developed by ISO/IEC SC1/JTC1 are identified by (T), indicating that final agreement has not been reached among the participating national bodies of SC1.

The following cross-references are used in this glossary:

Contrast with. This refers to a term that has an opposite or substantively different meaning.

See. This refers the reader to another keyword or phrase for the same term.

See also. This refers the reader to definite additional information contained in another entry.

A

access control

A list of all devices that can access other devices across the network and the permissions associated with that access. *See also* [persistent binding](#); [zoning](#).

active field-replaceable unit

Active FRU. A FRU that is currently operating as the active, and not the backup FRU. *See also* [backup field-replaceable unit](#).

active zone set

A single zone set that is active in a multiswitch fabric and is created when a specific zone set is enabled. This zone set is compiled by checking for undefined zones or aliases. *See also* [zone](#); [zone set](#).

AL_PA

See [arbitrated loop physical address](#).

arbitrated loop physical address

AL_PA. A 1-byte value used in the arbitrated loop topology that identifies loop ports (L_Ports). This value then becomes the last byte of the address identified for each public L_Port on the loop.

B

backup field-replaceable unit

Backup FRU. When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain director or switch and Fibre Channel link operation. *See also* [active field-replaceable unit](#).

backup FRU

See [backup field-replaceable unit](#).

beaconing

Use of light-emitting diodes (LEDs) on ports, port cards, field-replaceable units (FRUs), and directors to aid in the fault-isolation process. When enabled, active beaconing will cause LEDs to flash in order for the user to locate field-replaceable units (FRU's), switches, or directors in cabinets or computer rooms.

BB_Credit See [buffer-to-buffer credit](#).

blocked port In a director or switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

buffer Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. See [buffer-to-buffer credit](#).

buffer-to-buffer credit BB_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N_Port) or fabric port (F_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N_Port or F_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. BB_Credit can be adjustable to provide different levels of compensation.

C

channel A point-to-point link that transports data from one point to the other.

Class 2 Fibre Channel service Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N_Ports).

Class 3 Fibre Channel service Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N_Ports). *Synonymous with* [datagram](#).

Class F Fibre Channel service Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multiswitch fabric.

Class of Fibre Channel service Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

community profile Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

configuration data The collection of data that results from configuring product and system operating parameters. For example, configuring operating parameters, simple network management protocol (SNMP) agent,

zoning configurations, and port configurations through the Element Manager application, results in a collection of configuration data. Configuration data includes: identification data, port configuration data, operating parameters, simple network management protocol (SNMP) configuration, and zoning configuration.

connectionless Nondedicated link. Typically used to describe a link between nodes which allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast this to the dedicated bandwidth that is required in a Class 1 Fibre Channel Service point-to-point link.

connector *Synonym for optical fiber connector.*

control processor card CTP card. Circuit card that contains the director or switch microprocessor. The CTP card also initializes hardware components of the system after power-on. The card may contain an RJ-45 twisted pair connector.

control unit A hardware unit that controls the reading, writing, or displaying of data at one or more input/output units.

control unit port CUP. An internal director or switch port on the control processor (CTP) card (labelled FE) that communicates with channels to report error conditions and link initialization (D).

CRC *See [cyclic redundancy check](#).*

CTP card *See [control processor card](#).*

cyclic redundancy check CRC. System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

D

datagram *Synonym for [Class 3 Fibre Channel service](#).*

default Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified (D, I).

default zone A zone that contains all of the devices attached to a fabric that are not members of at least one of the zones of the activated zone set.

device (1) Mechanical, electrical, or electronic hardware with a specific purpose (*D*). *See also* [managed product](#).
(2) *See* [node](#).

dialog box A pop-up window in the user interface with informational messages or fields to be modified or completed with desired options.

domain A Fibre Channel term describing the most significant byte in the node port (N_Port) identifier for the Fibre Channel device. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

domain ID Domain identifier. A number that uniquely identifies a switch in a multiswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it will be granted by the principal switch and will become the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

domain name server In TCP/IP, a server program that supplies name-to-address translation by mapping domain name to internet addresses. (*D*)

E

E_D_TOV *See* [error-detect time-out value](#).

E_Port *See* [expansion port](#).

Element Manager application Application that implements the management user interface for a director or switch. (1) In your SAN management application, the software component that provides a graphical user interface for managing and monitoring switch products. When a product instance is opened from your SAN management application, the corresponding Element Manager application is invoked.

embedded web server	With director firmware Version 1.2 (or later) installed, administrators or operators with a browser-capable PC and an Internet connection can monitor and manage the director or switch through an embedded web server interface, called the SANpilot interface. The interface provides a GUI similar to the Element Manager application, and supports director configuration, statistics monitoring, and basic operation.
error-detect time-out value	E_D_TOV. The time the switch waits for an expected response before declaring an error condition.
error message	Indication that an error has been detected (<i>D</i>). <i>See also</i> information message ; warning message .
Ethernet	A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.
exchange fabric membership data	An SW_ILS that ensures that merging switches have the same fabric membership list during initialization.
expansion port	E_Port. Physical interface on a Fibre Channel switch within a fabric, that attaches to an E_Port on another Fibre Channel switch through an interswitch link (ISL) to form a multiswitch fabric. <i>See also</i> segmented E_Port.
F	
F_Port	<i>See</i> fabric port .
fabric	Entity that interconnects node ports (N_Ports) and is capable of routing (switching) Fibre Channel frames, using the destination ID information in the Fibre Channel frame header accompanying the frames. A switch is the smallest entity that can function as a complete switched fabric topology.
fabric binding	A security feature that limits the switches that can join a fabric, by specifying the WWN and Domain ID of the allowed switches in the fabric membership list.

fabric loop port	FL_Port. A fabric port (F_Port) that contains arbitrated loop (AL) functions associated with the Fibre Channel arbitrated loop (FC-AL) topology. The access point of the fabric for physically connecting an arbitrated loop of node loop ports (NL_Ports).
fabric port	F_Port. Physical interface within the fabric that connects to a node port (N_Port) through a point-to-point full duplex connection.
fabric membership list	The list of switches, specified by Domain ID and WWN, that will be exchanged during Exchange Fabric Membership Data.
failover	Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.
FAN	Fabric address notification.
FCP	A standard Fibre Channel protocol used to run SCSI over Fibre Channel.
fiber	The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.
Fibre Channel	FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.
Fibre Channel address	A 3-byte node port (N_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.
field-replaceable unit	FRU. Assembly removed and replaced in its entirety when any one of its components fails (<i>D</i>). <i>See</i> active field-replaceable unit .
firmware	Embedded program code that resides and runs on, for example, directors, switches, and hubs.
FL_Port	<i>See</i> fabric loop port .
FX_Port	A port configuration allowing a port to transition operationally to either an F_Port or an FL_Port. Only the Sphereon 4500 Switch supports the configuration of this port type.

FRU See [field-replaceable unit](#).

G

G_Port See [generic port](#).

gateway A multi-homed host used to route network traffic from one network to another, and to pass network traffic from one protocol to another.

gateway address (1) In transmission control protocol/Internet protocol (TCP/IP), a device that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a device sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

Gb/s Acronym for gigabits per second.

generic port G_Port. Physical interface on a director or switch that can function either as a fabric port (F_Port) or an expansion port (E_Port), depending on the port type to which it connects.

GPM See [G_Port Module](#).

G_Port Module An individual FRU that provides the physical attachment point for Fibre Channel devices.

Gx_Port A port configuration allowing a port to transition operationally to FL_Port as well as to the port operational states described for a G_Port. Only the Sphereon 4500 Switch supports the configuration of this port type.

H

hop (1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through it's destination point.

hop count The number of hops a unit of information traverses in a fabric.

hub (1) In Fibre Channel protocol, a device that connects nodes into a logical loop by using a physical star topology. (2) In Ethernet, a device used to connect the server platform and the directors or switches it manages.

I

information message Message notifying a user that a function is performing normally or has completed normally. *See also* [error message](#); [warning message](#).

initial program load IPL. The process of initializing the device and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

interface (1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two devices having different functions (*T*). (2) Hardware, software, or both, that link systems, programs, or devices (*D*).

Internet protocol IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer (*D*).

Internet protocol address IP address. Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a device on a network.

interoperability Ability to communicate, execute programs, or transfer data between various functional units over a network.

interswitch link ISL. Physical expansion port (E_Port) connection between two directors or switches in a fabric.

IP *See* [Internet protocol](#).

IP address *See* [Internet protocol address](#).

IPL *See* [initial program load](#).

ISL *See* [interswitch link](#).

L

LAN See [local area network](#).

LIN See [link incident](#).

link Physical connection between two devices on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

link incident LIN. Interruption to link due to loss of light or other causes. See also [link incident alerts](#).

link incident alerts A user notification, such as a graphic symbol in the Element Manager application *Hardware View* that indicates that a link incident has occurred. See also [link incident](#).

LIPS Loop Initialization Primitives. See [loop initialization primitive](#).

local area network LAN. A computer network in a localized geographical area (for example, a building or campus), whose communications technology provides a high-bandwidth medium to which many nodes are connected (*D*). See also [storage area network](#).

loopback test Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

loop initialization primitive LIP. In an arbitrated loop device, a process by which devices connected to hub ports (H_Ports) on the arbitrated loop device notify other devices and the switch of the presence in the loop by sending LIP sequences and subsequent frames through the loop. This process allows linked arbitrated loop devices to perform fabric loop port (FL_Port) arbitration as they link through hub ports.

M

managed product Hardware product that can be managed with the Element Manager application. McDATA directors and switches are managed products. See also [device](#).

multiswitch fabric A Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

N

N_Port See [node port](#).

name server (1) In TCP/IP, see [domain name server](#). (2) In Fibre Channel protocol, a server that allows node ports (N_Ports) to register information about themselves. This information allows N_Ports to discover and learn about each other by sending queries to the name server.

network address Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

node In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. See also [device](#).

node port N_Port. Physical interface within an end device that can connect to an fabric port (F_Port) on a switched fabric or directly to another N_Port (in point-to-point communications).

O

offline sequence OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

offline state When the switch or director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. Contrast with [online state](#).

OLS See [offline sequence](#).

online state When the switch or director is in the online state, all of the unblocked ports are allowed to log in to the fabric and begin communicating. Devices can connect to the switch or director if the port is not blocked and can communicate with another attached device if both devices are in the same zone, or if the default zone is enabled. *Contrast with [offline state](#).*

**operating state
(director or switch)**

The operating states are described as follows:

Online - when the director or switch is set online, an attached device can log in to the director if the port is not blocked. Attached devices can communicate with each other if they are configured in the same zone.

Offline - when the director or switch is set offline, all ports are set offline. The director or switch transmits the offline sequence (OLS) to attached devices, and the devices cannot log in to the director or switch.

operating state (port)

Valid states are:

- Online, offline, or testing.
- Beaconsing.
- Invalid attachment.
- Link incident or link reset.
- No light, not operational, or port failure.
- Segmented E_Port.

**optical fiber
connector**

Hardware component that transfers optical power between two optical fibers or bundles and is designed to be repeatedly connected and disconnected.

**out-of-band
management**

Transmission of management information, using frequencies or channels other than those routinely used for information transfer.

P

password

Unique string of characters known to the computer system and to a user who must specify it to gain full or limited access to a system and to the information stored within it.

path	In a network, any route between any two ports.
persistent binding	A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number. <i>See also</i> access control .
port	Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections (<i>D</i>).
port address name	A user-defined symbolic name of 24 characters or less that identifies a particular port address.
port card	Field-replaceable hardware component that provides the port connections for fiber cables and performs specific device-dependent logic functions.
port card map	Map showing port numbers and port card slot numbers inside a hardware cabinet.
port name	Name that the user assigns to a particular port through the Element Manager application.
preferred domain ID	Configured value that a switch will request from the Principal Switch. If the preferred value is already in use, the Principal Switch will assign a different value.
principal switch	In a multiswitch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

R

R_A_TOV	<i>See</i> resource allocation time-out value .
redundancy	Performance characteristic of a system or product whose integral components are backed up by identical components to which operations will automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hours/7 days per week) computer systems and networks.

resource allocation time-out value R_A_TOV. R_A_TOV is a value used to time-out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

S

SAN See [storage area network](#); system area network.

SAN management application (1) Software application that is the system management framework providing the user interface for managing Fibre Channel switch products. (2) The software application that implements the management user interface for all managed hardware products. The SAN management application can run both locally on a server platform and on a remote computer running client software.

SANpilot interface The interface provides a graphical user interface (GUI) similar to the Element Manager application, and supports director or switch configuration, statistics monitoring, and basic operations. With director or switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the director or switch through an embedded web server interface.

SBAR See [serial crossbar assembly](#).

segmented E_Port See [segmented expansion port](#).

segmented expansion port Segmented E_Port. E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins.

SEL System error light.

serial crossbar assembly SBAR. The assembly is responsible for Fibre Channel frame transmission from any director or switch port to any other director or switch port. Connections are established without software intervention.

serial port A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

server	A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.
simple network management protocol	SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.
simple network management protocol community	SNMP community. Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.
simple network management protocol community name	SNMP community name. The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent will only elicit a response if those queries are addressed with the correct SNMP community name.
simple network management protocol management station	SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.
SNMP	<i>See</i> simple network management protocol .
SNMP community	<i>See</i> simple network management protocol community .
SNMP community name	<i>See</i> simple network management protocol community name .
SNMP management station	<i>See</i> simple network management protocol management station .
storage area network	SAN. A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated. <i>See also</i> local area network .
subnet mask	A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move

the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

switch A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

switch binding A security method that limits the devices that can log in to a switch, by specifying the node WWN of the allowed devices in the Switch Membership List.

Switch Membership List The list of devices, specified by WWN, that can log in to a switch.

switch priority Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

T

telnet A protocol designed to provide general, bi-directional, eight-bit byte oriented communication. It is a standard method of interfacing terminal devices and terminal-oriented processes to each other.

topology The logical, physical, or both arrangement of stations on a network.

trap Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

U

UPM See [universal port module](#).

uniform resource locator URL. A URL is the address of a document or other resource on the Internet.

universal port module A flexible 1 gigabit-per-second or 2 gigabit-per-second module that contains four generic ports (G_Ports).

URL *See* [uniform resource locator](#).

user datagram protocol UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network.

W

warning message A message that indicates a possible error has been detected. *See also* [error message](#); [information message](#).

World Wide Names WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

WWN *See* [World Wide Names](#).

Z

zone Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot. *See also* [active zone set](#); [zone set](#); [zoning](#).

zone member Specification of a device to be included in a zone. A zone member can be identified by the port number of the director or switch to which it is attached or by its port World Wide Name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

zone set A collection of zones that may be activated as a unit. *See also* [active zone set](#); [zone](#).

zoning Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director or switch, may be configured into one or more zones. *See also* [access control](#); [zone](#).

Symbols

" 1-14
1-20
? 1-19

Numerics

60 characters in history log 1-13
80-column output 1-14

A

access control list 2-62
 adding a range 2-62
 delete a range 2-63
 disable 2-63
 enable 2-63
 show 2-64
access rights
 relationship to other products 1-16
active zoning configuration 2-92
add
 access control list 2-62
address
 port 2-28
alerts, threshold 2-116
ASCII character set 2-5
asynchronous commands 1-3
attached
 fabric binding terminology 2-52
audit log
 show 2-139
authentication
 configuring E port 2-34, 2-35

 configuring interface 2-34
 configuring N port 2-36
 configuring Open Systems 2-37, 2-38
 configuring outgoing 2-33
 configuring port 2-40
 configuring sequence 2-33
 configuring serial 2-38
 configuring Web 2-39
 showing settings 2-39
authorization traps, SNMP 2-69

B

back pressure state
 OpenTrunking 2-105
backslash 1-14
BB_credits
 configuring 2-26
beaconing
 port 2-95
 unit 2-96
block port 2-25

C

cable, replacing 1-22
case sensitivity 1-3
character set 2-5
class 2 counters 2-99
class 3 counters 2-100
CLI 1-2
 command tree 1-5
 ED-5000 Director 1-21
 errors, handling 1-18
 globally available commands 1-5

- help 1-19
- logging in or out 1-14
- lost 2-97
- navigation conventions 1-3
- output 1-14
- parameters 1-13
- purpose 1-2
- root> prompt 1-12
- using 1-2
- CLI commands, case sensitivity 1-3
- commaDelim command 1-17
 - globally available 1-5
- command line interface 1-2
 - command tree 1-5
 - ED-5000 1-21
 - errors, handling 1-18
 - globally available commands 1-5
 - help 1-19
 - logging in or out 1-14
 - lost 2-97
 - navigation conventions 1-3
 - output 1-14
 - parameters 1-13
 - purpose 1-2
 - root> prompt 1-12
 - using 1-2
- command tree 1-5
 - limitations on movements within 1-13
 - navigation of 1-12
- commands
 - asynchronous 1-3
 - commaDelim 1-17
 - config 2-5
 - ED-5000 1-21
 - login 1-15
 - logout 1-16
 - maint 2-95
 - name server information 2-158
 - perf 2-99
 - periods in 1-3
 - show 2-138
 - that take effect immediately 2-51, 2-84
- commenting scripts 1-20
- config command 2-5
- configuration data, resetting 2-95
- configuration, resetting 2-97
- congestion
 - unresolved 2-109
- congestion threshold
 - OpenTrunking 2-106
- connection loss, ethernet 1-22
- conventions
 - documentation 1-3
 - navigation 1-3
 - used in manual xvii
- counter data 2-99, 2-100
- counter threshold alert
 - activating 2-116
 - types 2-118
- counter threshold alerts 2-116
- CTA 2-116
- CUP zoning 2-17, 2-18

D

- data transfers, disruption of 2-29, 2-78
- date and time, system 2-82
- deactivate fabric binding 2-55
- default values, resetting 2-97
- default zone 2-92
- delete
 - access control list 2-63
 - preferred path 2-110
- disable
 - access control list 2-63
 - OpenTrunking 2-107
 - SNMP agent 2-71
- documentation conventions 1-3
- documentation, related xvi
- Domain ID
 - state 2-73
- domain ID, port member
 - adding 2-86
 - deleting 2-89
- domain RSCN state 2-72

E

- e_d_tov 2-73
- E_port, setting 2-31
- ED-5000 Director 1-21
- element managers
 - enabling Telnet 1-22
- Embedded Frame Log
 - show configuration 2-140

- view 2-142, 2-143
- enable
 - access control list 2-63
 - OpenTrunking 2-107
 - SNMP agent 2-71
- Enterprise Fabric Mode
 - activating 2-5, 2-6
 - deactivating 2-5, 2-6
- error counters, port 2-102
- error light, system, clearing 2-97
- escape character 1-14
- ethernet attributes 2-154
- ethernet cable, replacing 1-22
- ethernet connection, loss of 1-22
- event log 2-144
- exit port
 - set 2-111

F

- F frames
 - configuring logging 2-140
- F_port, setting 2-31
- fabric address notification (FAN)
 - setting state 2-25
- fabric binding
 - activate 2-53
 - active configuration 2-56
 - active FBML
 - show 2-56
 - add members 2-53, 2-54
 - deactivate 2-55
 - delete members 2-55
 - membership list 2-54
 - delete member 2-55
 - online state functions 2-52
 - pending configuration
 - activate 2-53
 - add attached members 2-53
 - pending FBML
 - show 2-57
 - replace pending 2-56
 - replace pending FBML 2-56
 - security 2-51
 - show 2-180
 - show pending 2-57
 - terms

- attached 2-52
 - local 2-52
 - unattached 2-52
- fabric binding membership list
 - active 2-56
 - add member 2-54
 - clear 2-54
 - deactivate 2-55
 - delete member 2-55
 - pending
 - show 2-57
 - replace pending FBML 2-56
- fabric log
 - view 2-145, 2-146
- fabric nodes
 - list 2-148
 - show 2-148
- fabric topology
 - list 2-149
 - show 2-149
- factory settings, resetting 2-95, 2-97
- feature
 - Enterprise Fabric Mode 2-5, 2-6
 - FICON Management Server 2-6, 2-19
 - list 2-150
 - NPIV 2-8
 - Open Systems Management Server 2-8, 2-24
 - OpenTrunking 2-8, 2-107
 - SANtegrity 2-5, 2-6
 - show 2-150
- feature keys 2-7
 - resetting 2-97
- features
 - preferred path 2-110
- fencing policies
 - show 2-150
- Fibre Alliance MIB
 - SNMP 2-70
- FICON CUP
 - show zoning 2-152
 - zoning 2-17, 2-18
- FICON Management Server 2-6, 2-7, 2-19
- FICON MS
 - show 2-152
- ficonms 2-6, 2-19
- FRU information 2-153

G

G_port, setting [2-31](#)
 gateway address [2-21](#)
 globally available commands [1-5](#)
 graphical user interface [1-2](#)
 GUI [1-2](#)
 enabling Telnet [1-22](#)

H

help command [1-19](#)
 help, technical support [xvii](#)
 history log [1-13](#)
 clearing [1-13](#)
 HTTP [1-2](#)

I

inactive operational state [2-176](#)
 inactive state reasons [2-175](#)
 insistent Domain ID
 state [2-73](#)
 interactive interfaces [1-2](#)
 interoperability mode [2-74](#)
 invalid attachment state reasons [2-175](#)
 IP address, ethernet [2-20](#)
 IP configuration, showing [2-21](#)
 IP line speed, ethernet [2-21](#)
 IPL [2-97](#)

K

keys
 for feature sets [2-7](#)
 resetting [2-97](#)

L

Latin-1 character set [2-5](#)
 limitations, history log [1-13](#)
 limited fabric RSCN [2-74](#)
 link counters [2-104](#)
 link incident log [2-154](#)
 link sequence counts [2-120](#)
 local
 fabric binding terminology [2-52](#)
 log
 Embedded Frame

 settings [2-140](#)
 threshold alert [2-192](#)
 view [2-144](#)
 logging in [1-14](#)
 logging out [1-14](#)
 logical link errors [2-120](#)
 login command [1-15](#)
 globally available [1-5](#)
 login server [2-155](#)
 logout command [1-16](#)
 globally available [1-5](#)
 low BB credit threshold [2-106](#)

M

maint command [2-95](#)
 Management Style
 FICON [2-7](#)
 manual
 conventions [xvii](#)
 using this [xvi](#)
 McDATA
 product publications, ordering [xviii](#)
 technical support [xvii](#)
 web site [xvi](#)
 membership list
 fabric binding [2-55](#)
 add attached [2-53](#)
 add member [2-54](#)
 clear [2-54](#)
 switch binding [2-64](#)

N

name server [2-156, 2-158](#)
 names, for ports [2-26](#)
 navigating the command tree [1-12](#)
 faster methods [1-12](#)
 limitations [1-13](#)
 navigation conventions [1-3](#)
 NPIV
 configuring port IDs [2-22](#)
 disable [2-8](#)
 enable [2-8](#)
 set state [2-8](#)
 setting state [2-23](#)
 showing configuration [2-23](#)
 null strings [1-14](#)

NV-RAM configuration parameters, reset [2-97](#)

O

offline, setting switches for configuration [2-72](#)

Open Systems

setting state [2-24](#)

Open Systems Management Server [2-8](#), [2-24](#)

OpenTrunking

back pressure state [2-105](#)

congestion threshold [2-106](#)

low BB credit threshold [2-106](#)

show [2-108](#)

configuration [2-161](#)

reroute log [2-162](#)

state [2-8](#), [2-107](#)

unresolved congestion [2-109](#)

operational state [2-175](#)

ordering product publications [xviii](#)

OSMS state [2-8](#), [2-24](#)

output [1-14](#)

commaDelim command [1-17](#)

order of displayed values [1-11](#)

P

parameters [1-13](#)

passwords

format [1-14](#)

perf command [2-99](#)

performance alerts [2-116](#)

performance services [2-99](#)

periods in command names [1-3](#)

physical link errors [2-120](#)

port

address, show [2-173](#)

beaconing [2-95](#)

binding [2-57](#), [2-182](#)

binding,state [2-57](#)

block [2-25](#)

configuration [2-163](#)

configuration, show [2-171](#)

configuring BB_credits [2-26](#)

configuring WWN, binding [2-59](#)

error counters [2-102](#)

IDs, NPIV [2-22](#)

information [2-166](#)

link counters [2-104](#)

name [2-26](#)

nodes [2-167](#)

optical diagnostics [2-169](#)

port statistics [2-102](#)

port technology information [2-177](#)

resetting [2-96](#)

show configuration [2-163](#)

show exit [2-164](#)

show nodes [2-167](#)

show optic [2-170](#)

showing address configuration [2-28](#)

showing authentication state [2-41](#)

showing configuration [2-27](#)

speed [2-29](#)

statistics, clearing [2-102](#)

status [2-174](#)

swapping [2-30](#)

threshold alert [2-121](#), [2-122](#)

traffic counters [2-136](#)

type [2-31](#)

port binding state [2-57](#)

port number, zone member

adding [2-86](#)

deleting [2-89](#)

port statistics, resetting [2-102](#)

pound sign [1-20](#)

preferred domain ID [2-75](#)

preferred path

clear [2-110](#)

delete [2-110](#)

destination [2-113](#), [2-178](#)

disable [2-112](#)

enable [2-112](#)

feature overview [2-110](#)

set exit port [2-111](#)

show [2-178](#)

show exit port [2-164](#)

show path [2-113](#)

show state [2-115](#)

source port [2-113](#), [2-178](#)

state [2-112](#)

principal switch [2-76](#)

priority, of switches [2-75](#)

publications

McDATA products, ordering [xviii](#)

related [xvi](#)

updates [xvi](#)

Q

quotation marks
 for spaces 1-14
 in strings 1-14

R

r_a_tov 2-76
 RADIUS server
 adding 2-43
 configuring deadtime 2-42
 configuring timeout 2-45
 deleting 2-43
 showing configuration 2-44
 range
 access control list 2-62, 2-63
 registered trademarks xix
 related documentation xvi
 reroute log, OpenTrunking 2-162
 rerouting delay 2-77
 root, transitioning through 1-12
 root> prompt 1-12
 RSCN
 fabric 2-74
 zoning state 2-81

S

SANtegrity
 Enterprise Fabric Mode 2-5, 2-6
 scripting environments 1-2
 scripts, commenting 1-20
 secret
 setting 2-45
 secrets
 format 1-14
 secure shell
 keys 2-61
 set state 2-61
 show state 2-61
 security
 adding RADIUS server 2-43
 adding users to database 2-46
 configuring 2-32
 configuring authentication interface 2-34
 configuring authentication sequence 2-33
 configuring E port authentication 2-34, 2-35

 configuring N port authentication 2-36
 configuring Open Systems authentication 2-37, 2-38
 configuring outgoing authentication 2-33
 configuring port state 2-40
 configuring RADIUS server deadtime 2-42
 configuring serial authentication 2-38
 configuring transmission attempts 2-42
 configuring users 2-46
 configuring Web authentication 2-39
 deleting RADIUS server 2-43
 deleting users from database 2-47
 fabric binding 2-51
 activate 2-53
 active configuration 2-56
 add members 2-53, 2-54
 deactivate 2-55
 delete members 2-55
 replace pending 2-56
 show pending 2-57
 modifying users 2-48
 port binding 2-57
 reset SSH keys 2-61
 set SSH state 2-61
 setting secret 2-45
 setting user role 2-49
 show SSH state 2-61
 showing port 2-41
 showing RADIUS server 2-44
 showing state 2-39
 showing user 2-50
 switch binding 2-64
 adding member 2-65
 deleting member 2-66
 setting state 2-66
 showing configuration 2-67
 timeout
 RADIUS server 2-45
 security log 2-181
 segmented E_Port 2-175
 segmented E_port
 state reasons 2-175
 service, technical support xvii
 setting online or offline 2-98
 settings
 threshold alert settings 2-135
 show

- access control list 2-64
- all 2-138
- ethernet attributes 2-154
- event log 2-144
- fabric binding 2-180
- fabric nodes 2-148
- fabric topology 2-149
- features list 2-150
- fencing policies 2-150
- FICON CUP zoning 2-152
- FICON MS 2-152
- FRU information 2-153
- link incident log 2-154
- login server 2-155
- name server 2-156
- open trunking configuration 2-161
- OpenTrunking
 - configuration 2-161
 - rerouteLog 2-162
- OpenTrunking information 2-108
- port address 2-173
- port binding for all ports 2-182
- port configuration 2-163, 2-171
- port exit 2-164
- port information 2-166
- port nodes 2-167
- port optic 2-170
- port optical diagnostics 2-169
- port status 2-174
- port technology information 2-177
- preferred path 2-178
- preferred path exit port 2-164
- security log 2-181
- switch access control list 2-183
- switch attributes 2-186
- switch binding 2-184
- Switch Binding Membership List 2-68
- system attributes 2-188
- threshold alert list 2-189
- threshold alert log 2-192
- threshold alert settings 2-135
- WWN 2-148
- show commands
 - active zoning configuration 2-92
 - all 2-138
 - configuration for port 2-27
 - features 2-9
 - order of output 1-11
 - pending zoning configuration 2-93
 - port
 - show binding 2-58
 - show branch 2-138
 - SNMP configuration
 - config.snmp.show 2-71
 - snmp.show 2-185
 - switch configuration 2-78
 - system configuration 2-83
- SNMP
 - authorization traps 2-69
 - community
 - adding 2-68
 - deleting 2-70
 - disable agent 2-71
 - enable agent 2-71
 - Fibre Alliance MIB version 2-70
 - set state 2-71
- spaces, quotation marks required 1-14
- speeds
 - port 2-29
 - switches 2-78
- state
 - back pressure 2-105
 - OpenTrunking 2-8, 2-107
 - setting NPIV 2-23
 - SNMP 2-71
 - Zone Flex Pars 2-80
 - zoning RSCN 2-81
- statistic table, threshold alert 2-126
- statistics, port, clearing 2-102
- strings, null 1-14
- strings, quotation marks in 1-14
- subnet mask 2-21
- summed sets 2-120
- swap ports
 - by address 2-30
 - by number 2-30
- switch attributes, displaying 2-186
- Switch Binding
 - add SBML member 2-65
 - configuration 2-64
 - delete SBML member 2-66
 - show configuration 2-67
- switch binding 2-184
 - adding member 2-65

- delete member 2-66
- online state functions 2-65
- set state 2-66
- show configuration 2-67
- show SBML 2-68
- Switch Binding Membership List 2-68
 - add member 2-65
 - delete member 2-66
 - overview 2-64
 - show 2-68
- switches 2-98
 - configuring IP address 2-20
 - configuring IP line speed 2-21
 - configuring, set offline 2-72
 - e_d_tov 2-73
 - event log 2-144
 - FRU information 2-153
 - interoperability mode 2-74
 - IPL 2-97
 - login server database 2-155
 - name server database 2-156, 2-158
 - preferred domain ID 2-75
 - principal 2-76
 - priority 2-75
 - r_a_tov 2-76
 - rerouting delay 2-77
 - security log 2-181
 - showing LAN configuration 2-21
 - speed 2-78
 - system contact 2-81
 - system description 2-82
 - system location 2-83
 - system name 2-83
- system attributes, displaying 2-188
- system contact attribute 2-81
- system date and time 2-82
- system description 2-82
- system error light, clearing 2-97
- system location 2-83
- system name 2-83

T

- tabular output 1-17
- technical support xvii
- Telnet client session 1-2
 - connection, loss of 1-22

- threshold alert
 - activate 2-127
 - add alert 2-120
 - add port 2-130
 - add throughput alert 2-129
 - alert list 2-189
 - counter
 - setting 2-123
 - deactivate 2-127
 - delete alert 2-127
 - disable 2-127
 - enable 2-127
 - list 2-189
 - log 2-192
 - name 2-125
 - parameters 2-124, 2-134
 - port
 - add 2-121, 2-130
 - remove 2-122, 2-131
 - remove port 2-131
 - set parameters 2-134
 - settings
 - show 2-135
 - show 2-127, 2-135
 - show utilization types 2-135
 - statistic table, show 2-126
 - throughput
 - add alert 2-129
 - trigger
 - percentage 2-133
 - trigger type 2-132
 - utilization percentage 2-133
 - utilization type 2-132
 - utilization types 2-135
- threshold alerts
 - overview 2-116
 - summed sets 2-120
- throughput alert
 - add 2-129
 - port 2-130, 2-131
 - set parameters 2-134
 - show settings 2-135
 - show utilization types 2-135
 - utilization percentage 2-133
 - utilization type 2-132
- Throughput Threshold Alert
 - activating 2-117

throughput threshold alert [2-116](#)
 types [2-118](#)
 time, system [2-82](#)
 trademarks [xix](#)
 traffic counters [2-136](#)
 traversing the command tree [1-12](#)
 trunking
 congestion [2-106, 2-109](#)
 TTAs [2-116](#)
 types, port [2-31](#)

U

UDP [2-69, 2-72, 2-185](#)
 unattached
 fabric binding terminology [2-52](#)
 unit beaconing [2-96](#)
 unresolved congestion
 OpenTrunking [2-109](#)
 up-arrow command [1-13](#)
 user
 adding to database [2-46](#)
 configuring [2-46](#)
 deleting from database [2-47](#)
 modifying [2-48](#)
 setting role [2-49](#)
 showing [2-50](#)
 user access rights [1-14](#)
 relationship to other products [1-16](#)
 user datagram protocol [2-69, 2-72, 2-185](#)
 using this manual [xvi](#)
 utilization type
 threshold alert [2-132](#)

V

view
 logs [2-142, 2-143, 2-145, 2-146](#)

W

web site, McDATA [xvi, xviii](#)
 web-based interface [1-2](#)
 enabling Telnet [1-22](#)
 work area [2-84](#)
 world-wide name members
 adding [2-87](#)

 deleting [2-90](#)
 wrap count [2-99, 2-100](#)
 WWN
 port binding [2-59](#)
 show [2-148](#)
 WWN members
 adding [2-87](#)
 deleting [2-90](#)

Z

zone
 adding [2-87](#)
 default state [2-92](#)
 deleting [2-90](#)
 members
 adding by port [2-86](#)
 adding by WWN [2-87](#)
 deleting by port [2-89](#)
 deleting by WWN [2-90](#)
 renaming [2-91](#)
 Zone Flex Pars
 zoning state [2-80](#)
 zone members
 clearing [2-88](#)
 domain ID
 adding [2-86](#)
 deleting [2-89](#)
 zone set
 activating to fabric [2-84, 2-85](#)
 clearing [2-88](#)
 deactivating [2-89](#)
 renaming [2-91](#)
 replacing [2-92](#)
 temporary copy [2-84](#)
 zone sets and zones
 displaying [2-85](#)
 zoning
 configuring [2-84](#)
 FICON CUP [2-17, 2-18](#)
 RSCN state [2-81](#)
 show FICON CUP [2-152](#)
 Zone Flex Pars state [2-80](#)
 zoning configuration
 active, display [2-92](#)
 pending, display [2-93](#)

